

PCT

世界知的所有権機関
国際事務局

特許協力条約に基づいて公開された国際出願



(51) 国際特許分類6 H04N 7/16, 7/167, 7/08, H04K 1/04, H04L 12/18	A1	(11) 国際公開番号 WO00/03541 (43) 国際公開日 2000年1月20日(20.01.00)
(21) 国際出願番号 PCT/JP98/03127 (22) 国際出願日 1998年7月13日(13.07.98) (71) 出願人 (米国を除くすべての指定国について) ソニー株式会社(SONY CORPORATION)[JP/JP] 〒141-0001 東京都品川区北品川6丁目7番35号 Tokyo, (JP) (72) 発明者 ; および (75) 発明者 / 出願人 (米国についてのみ) 窪田達也(KUBOTA, Tatsuya)[JP/JP] 若槻典生(WAKATSUKI, Norio)[JP/JP] 〒141-0001 東京都品川区北品川6丁目7番35号 ソニー株式会社内 Tokyo, (JP) (74) 代理人 弁理士 田辺恵基(TANABE, Shigemoto) 〒150-0001 東京都渋谷区神宮前1丁目11番11-508号 グリーンフアンタジアビル5階 Tokyo, (JP)	(81) 指定国 JP, KR, US, 欧州特許 (CY, DE, FR, GB, IT, NL) 添付公開書類 国際調査報告書	

(54) Title: DATA MULTIPLEXER, PROGRAM DISTRIBUTION SYSTEM, PROGRAM TRANSMISSION SYSTEM, TOLL BROADCAST SYSTEM, PROGRAM TRANSMISSION METHOD, LIMITED RECEIVING SYSTEM, AND DATA RECEIVER

(54) 発明の名称 データ多重化装置、プログラム配信システム、プログラム伝送システム、有料放送システム、プログラム伝送方法、限定受信システム及びデータ受信装置

Program number	Video	Main Audio	Sub Audio	Private
1	Ks 1		---	---
2	Ks 2	Ks 3	Ks 4	
3	Ks 5	Ks 6	---	---
4	Ks 7	Ks 8	Ks 9	Ks 10
5		Ks 11		
6	Ks 12		---	---
7	Ks 13		Ks 14	
8	Ks 15			
9	Ks 16	Ks 17	Ks 18	Ks 19

(57) Abstract

A data multiplexer, a program distribution system, a program transmission system, a toll broadcast system, a program transmission method, a limited receiving system, and a data receiver for transmitting transport stream packets of program data comprising a plurality of data elements having a transport stream packet structure, wherein a viewer can make a reception contract for each data element by generating a scramble key Ks corresponding to one or more data elements out of the data elements constituting one program and performing scrambling for each data element.

(57)要約

トランSPORTストリームパケット構成の複数のデータエレメントからなるプログラムデータの各トランSPORTストリームパケットを多重化して送信するデータ多重化装置、プログラム配信システム、プログラム伝送システム、有料放送システム、プログラム伝送方法、限定受信システム及びデータ受信装置において、1つのプログラムを構成する複数のデータエレメントのうち、1つ又は複数のデータエレメントに対応したスクランブルキーKsを生成し、各データエレメントごとにスクランブルをかけるようにすることにより、視聴者はデータエレメントごとに視聴契約を結ぶことができる。

PCTに基づいて公開される国際出願のパンフレット第一頁に掲載されたPCT加盟国を同定するために使用されるコード(参考情報)

AE アラブ首長国連邦	DM ドミニカ	KZ カザフスタン	RU ロシア
AL アルバニア	EE エストニア	LC セントルシア	SD スーダン
AM アルメニア	ES スペイン	LI リヒテンシュタイン	SE スウェーデン
AT オーストリア	FI フィンランド	LK スリランカ	SG シンガポール
AU オーストラリア	FR フランス	LR リベリア	SI スロヴェニア
AZ アゼルバイジャン	GA ガボン	LS レソト	SK スロヴァキア
BA ボスニア・ヘルツェゴビナ	GB 英国	LT リトアニア	SL シエラ・レオネ
BB バルバドス	GD グレナダ	LU ルクセンブルグ	SN セネガル
BE ベルギー	GE グルジア	LV ラトヴィア	SZ スワジランド
BF ブルガリア・ファーン	GH ガーナ	MA モロッコ	TD チャード
BG ブルガリア	GM ガンビア	MC モナコ	TG トーゴ
BJ ベナン	GN ギニア	MD モルドバ	TJ タジキスタン
BRL ブラジル	GW ギニア・ビサオ	MG マダガスカル	TZ タンザニア
BY ベラルーシ	GR ギリシャ	MK マケドニア旧ユーゴスラヴィア	TM トルクメニスタン
CA カナダ	HR クロアチア	共和国	TR トルコ
CF 中央アフリカ	HU ハンガリー	ML マリ	TT トリニダッド・トバゴ
CG コンゴ	ID インドネシア	MN モンゴル	UA ウクライナ
CH スイス	IE アイルランド	MR モーリタニア	UG ウガンダ
CI コートジボアール	IL イスラエル	MW マラウイ	US 米国
CM カメルーン	IN インド	MX メキシコ	UZ ウズベキスタン
CN 中国	IS アイスランド	NE ニジニエール	VN ヴィエトナム
CR コスタ・リカ	IT イタリア	NL オランダ	YU ユーロスマリビア
CU キューバ	JP 日本	NO ノルウェー	ZA 南アフリカ共和国
CY キプロス	KE ケニア	NZ ニュージーランド	ZW ジンバブエ
CZ チェコ	KG キルギスタン	PL ポーランド	
DE ドイツ	KP 北朝鮮	PT ポルトガル	
DK デンマーク	KR 韓国	RO ルーマニア	

明細書

データ多重化装置、プログラム配信システム、プログラム伝送システム、有料放送システム、プログラム伝送方法、限定受信システム及びデータ受信装置

技術分野

本発明はデータ多重化装置、プログラム配信システム、プログラム伝送システム、有料放送システム、プログラム伝送方法、限定受信システム及びデータ受信装置に関し、例えばビデオデータやオーディオデータを圧縮符号化し、多重化して伝送するデジタル放送システムのデータ多重化装置及びデータ受信装置に適用して好適なものである。

背景技術

近年、MPEG2 (Moving Picture Experts Group Phase 2) を用いてビデオデータやオーディオデータを圧縮符号化し、その符号化されたストリームを地上波や衛星波を利用して放送するデジタル放送システムが提案されている。このデジタル放送システムは、符号化されたビデオストリーム及び符号化されたオーディオストリーム等から構成される複数の各プログラムについて、各プログラムのビデオデータやオーディオデータ等のエレメンタリデータを所定バイト単位で分割し、その分割された各データの先頭にヘッダを加えることにより複数のトランSPORTパケットを生成する。そしてこのトランSPORTパケットを多重化し、地上波や衛星波を利用して送信する。

受信装置では、トランSPORTパケットを多重化してなる伝送データを受信すると、この受信されたデータから各トランSPORTパケットのヘッダ情報を読み出し、このヘッダ情報に基づいて多重化される前のエレメンタリデータを復元することにより、各プログラムの符号化されたビデオストリーム及び符号化されたオ

ーディオストリーム等を得る。

このようなデジタル放送システムにおいて、一般的に、1つのプログラムは複数のデータエレメント（ビデオデータと複数チャンネルのオーディオデータ）から構成されている。このようなデジタル放送システムにおいて、1つのプログラムの中に含まれるデータエレメント毎に、視聴者が契約を行うことが望まれている。例えば、1つのプログラムが、ビデオデータ、メインオーディオデータ、サブオーディオデータ、及び付加データ等の合計4つのデータエレメントから構成されている場合を想定する。従来のデジタル放送システムでは、1つのプログラム毎に契約を行っていた、つまり、6つのデータエレメント全てと契約しなければいけなかった。つまり、受信者がビデオデータとメインオーディオデータのみを契約したいと思っても、不必要的残りのエレメント（サブオーディオと付加データ）までも契約しなければいけないという問題があった。

また、従来のスクランブル装置は、多重化する前に行われていたので、プログラム毎のスクランブル装置が必要であり、装置の構成が大きくなる問題があった。

さらに、従来のデジタル放送システムでは、番組契約情報や暗号解読キーを一定の期間毎にプログラムに多重化して伝送していた。多重化されたストリームのビットレートの上限は制限されているので、番組契約情報や暗号解読キーを伝送する分だけ、プログラムの伝送レートを確保できない場合がある。伝送レートを十分確保できないときには、いずれかのプログラムデータをバッファリングする伝送バッファがオーバーフローしてしまうという問題を有していた。

発明の開示

本発明は、そのような点を鑑みてなされた発明であって、受信者がプログラムを構成するデータエレメントのうち必要なデータエレメントのみを受信できるような、つまり、データエレメント毎にスクランブルをかけることのできるデジタル放送システムを提案するものである。

また、本発明は、プログラム毎にスクランブル装置を設ける構成を回避して装置構成を小型化することのできるデジタル放送システムを提案するものである。

また、本発明は、いずれかのプログラムデータをバッファリングする伝送バッファのオーバーフローを回避し得るデジタル放送システムを提案するものである。

かかる課題を解決するため本発明においては、トランSPORTストリームパケット構成の複数のデータエレメントからなるプログラムデータの上記各トランSPORTストリームパケットを多重化して送信するデータ多重化装置において、データエレメントごとに対応するスクランブルキーを生成するスクランブルキー生成手段と、スクランブルキー生成手段によって生成されたスクランブルキーを用いて対応する上記データエレメントのトランSPORTストリームパケットにスクランブルをかけるスクランブル手段とを備え、1つのプログラムを構成する複数のデータエレメントのうち、1つ又は複数のデータエレメントに対応したスクランブルキーを生成し、各データエレメントごとにスクランブルをかけるようにする。

各データエレメントごとにスクランブルをかけることにより、視聴者はデータエレメントごとに視聴契約を結ぶことができる。

また本発明においては、複数のデータエレメントから構成されるプログラムを配信するプログラム配信システムにおいて、プログラム毎及びデータエレメント毎の顧客の契約を顧客管理システムによって管理すると共に、プログラムに含まれるデータエレメントをデスクランブルする際に使用するスクランブルキーをデータエレメント毎に生成し、生成されたスクランブルキーに基づいて、多重化ストリームに含まれる符号化データエレメントに対して各データエレメント毎に選択的にスクランブルをかけることにより、視聴者は各データエレメント毎に視聴契約を結ぶことができる。

また本発明においては、複数のデータエレメントから構成されるプログラムを伝送するプログラム伝送システムにおいて、顧客が契約したプログラム及びデータ

タエレメントのみを視聴できるように、プログラムに含まれる複数のデータエレメントをスクランブルする際に使用される複数のスクランブルキーを生成し、当該生成されたスクランブルキーに基づいて各データエレメント毎に選択的にスクランブルをかけ、当該スクランブルがかけられたデータエレメントを多重化して伝送することにより、視聴者は各データエレメント毎に視聴契約を結び、その契約されたデータエレメントのみをスクランブル解除して視聴することができる。

また本発明においては、複数のデータエレメントから構成されるプログラムを放送する有料放送システムにおいて、プログラム毎及びデータエレメント毎の顧客の契約を顧客管理システムによって管理すると共に、プログラムに含まれるデータエレメントをデスクランブルする際に使用するスクランブルキーをデータエレメント毎に生成し、生成されたスクランブルキーに基づいて、多重化ストリームに含まれる符号化データエレメントに対して各データエレメント毎に選択的にスクランブルをかけることにより、視聴者は各データエレメント毎に視聴契約を結ぶことができる。

また本発明においては、プログラム配信システムから配信された複数のプログラム及び当該プログラムを構成する複数のデータエレメントのうち、契約されたプログラム及びデータエレメントのみを限定的に受信する限定受信システムにおいて、複数の暗号化スクランブルキーを含んだ複数のトランSPORTストリームパケットから、受信者が契約したプログラム及びデータエレメントに関連付けられた暗号化スクランブルキーを含んだトランSPORTストリームパケットをフィルタリングし、当該フィルタリングされた複数のトランSPORTストリームパケットに含まれる複数の暗号化スクランブルキーの暗号を解読し、暗号解読された複数のスクランブルキーを生成し、複数のデータエレメントに対応付けられた複数の暗号解読されたスクランブルキーを使用して複数のデータエレメント毎にデスクランブルすることにより、視聴者は各データエレメント毎に視聴契約を結び、その契約されたデータエレメントのみをスクランブル解除して視聴することができる。

また本発明においては、多重化された各トランSPORTストリームパケットに対してそれぞれ対応するスクランブルキーを用いてスクランブルをかけることにより、各トランSPORTストリームパケットを多重化する前にスクランブルをかける場合に比べて、スクランブルをかけるための回路構成が簡単になる。

また本発明においては、複数のデータエレメントを構成する複数のパケットデータを格納する複数のバッファメモリと、バッファメモリを切り換えるスイッチ手段を有し、当該スイッチ手段によつてバッファメモリを順次時分割に切り換えることによつて複数のパケットデータ列を時分割に多重化して出力する多重化手段と、スイッチ手段による切り換え対象である複数のバッファメモリを、パケットデータ列の入力レートに応じて選択するスイッチ制御手段とを備え、入力レートが基準レートに比べて高いとき、複数のバッファメモリのうち、優先順位の低い情報をバッファリングするバッファメモリを切り換え対象から除外してスイッチ手段を切り換え制御することにより、優先順位の高いデータエレメントをバッファリングするバッファメモリがオーバーフローすることを未然に防止し得る。

また本発明においては、トランSPORTストリームパケット構成の複数のデータエレメントからなるプログラムデータの各トランSPORTストリームパケットを多重化してなる多重化データを受信するデータ受信装置において、データエレメントごとに対応するスクランブルキーを多重化データから抽出するスクランブルキー抽出手段と、スクランブルキー抽出手段によつて抽出されたスクランブルキーを用いて多重化データに含まれる各データエレメントごとのトランSPORTストリームパケットをデスクランブルするデスクランブル手段とを備え、スクランブルキーを用いて当該スクランブルキーに対応するデータエレメントごとにそのトランSPORTストリームパケットをデスクランブルすることにより、データエレメントごとに個別にスクランブルを解除することができる。

図面の簡単な説明

図1は、本発明によるデジタル放送システムの構成を示すブロック図である。

図 2 は、各プログラムに含まれるエレメンタリデータとスクリプブルキーとの対応を示す略線図である。

図 3 は、トランSPORTストリームパケットに記録される情報とその P I D 値との対応を示す略線図である。

図 4 は、トランSPORTパケットの種類とその P I D 値との対応を示す略線図である。

図 5 は、エンコーディングシステムの構成を示すプロツク図である。

図 6 は、トランSPORTパケットのシンタックスを示す略線図である。

図 7 は、トランSPORTパケットのシンタックスを示す略線図である。

図 8 は、トランSPORTパケットのシンタックスを示す略線図である。

図 9 は、トランSPORTパケットのシンタックスを示す略線図である。

図 10 は、マルチプレクサシステムの構成を示すプロツク図である。

図 11 は、各テーブルとその P I D との対応を示す略線図である。

図 12 は、 program association section のシンタックスを示す略線図である。

図 13 は、 program association section のシンタックスを示す略線図である。

図 14 は、各セクションとその P I D 値との対応を示す略線図である。

図 15 は、 program map section のシンタックスを示す略線図である。

図 16 は、 program map section のシンタックスを示す略線図である。

図 17 は、 conditional access section のシンタックスを示す略線図である。

図 18 は、 conditional access section のシンタックスを示す略線図である。

図19は、conditional access descriptorのシンタックスを示す略線図である。

図20は、各テーブルによって表されるエレメンタリデータのP I Dと、descriptorの内容を示す略線図である。

図21は、EMMパケットのデータ構成を示す略線図である。

図22は、ECMパケットのデータ構成を示す略線図である。

図23は、受信装置の構成を示すブロック図である。

発明を実施するための最良の形態

以下、図面について本発明の一実施例を詳述する。

図1を参照して、本発明のデータ多重化装置が適用されるデータ放送システムに関して説明する。

このデータ放送システムは、衛星デジタル放送システムや地上波デジタル放送システムなどの有料の放送システムにおいて使用されるシステムであって、図1に示すように、放送番組編成システムB D P S (Broadcast_Data_Processing_System) 1と、顧客管理システムS M S (Subscriber_Management_System) 2と、顧客視聴許可システムS A S (Subscriber_Authorization_System) 3と、E P G (Electronic_Program_Guide) システム4と、サーバシステム5と、ルーティングシステム6と、エンコーディングシステム7と、マルチプレクサシステム8と、エンコーダ／マルチプレクサコントロールユニット9と、変調回路10とから構成されている。

放送番組編成システム1は、顧客管理システム2、顧客視聴許可システム3、E P G システム4、サーバシステム5、ルーティングシステム6、エンコーディングシステム7、マルチプレクサシステム8、エンコーダ／マルチプレクサコントロールユニット9及び変調回路10等の放送局に設けられている全てのシステム及び装置を統括的に管理するためのシステムである。この放送番組編成システ

ム 1 には、番組供給会社から供給された番組素材及びプロモーション素材や自局で作成した番組素材や C M 素材などのあらゆる素材の放映時間を管理するための番組編成表が登録されており、放送番組編成システム 1 は、この番組編成表に従って、各装置及びシステムを制御する。この番組編成表は、例えば、番組供給会社に関する情報などが記録されているサービス情報ファイル、1 時間単位又は 1 日単位の放送番組スケジュールが記録されているイベント情報ファイル、及び 1 5 秒単位の放送番組のタイムスケジュールが記録されている運行情報ファイル等から構成されている。

顧客管理システム 2 は、顧客登録情報や料金徴収情報等の顧客管理に関する情報を管理するためのシステムである。具体的には、この顧客管理システム 2 は、顧客の番組契約、課金、請求を中心とする有料放送システムの中核システムである。さらにこの顧客管理システム 2 は、データエレメントをスクランブルするためのスクランブルキー K_s を暗号化するためのワークキー K_w 等の鍵に関する情報や、委託放送事業者や番組供給会社や番組作成代理店の管理を行うための機能を有している。また、この顧客管理システム 2 は、受信側に設けられた I R D から電話回線を通じて供給される視聴情報をリアルタイムに処理する機能を有している。また、この顧客管理システム 2 は、後述する顧客視聴許可システム 3 に対して、視聴者の契約に関する契約情報やワークキー K_w に関する情報が格納された E M M (E n t i t l e m e n t _ M a n a g e m e n t _ M e s s a g e) データを供給する。この E M M データについては詳しくは後述する。

顧客視聴許可システム 3 は、顧客管理システム 2 から受け取った E M M データに含まれるワークキー K_w を、マスターキー K_m を使用して所定の暗号化アルゴリズムにて暗号化することによって、暗号化されたワークキー K_w' を生成する。尚、本発明のデジタル放送システムで用いられている暗号化アルゴリズムは、当社が開発した暗号化アルゴリズム C R Y P S (ソニー登録商標) という暗号化アルゴリズムであって、米国商務省で定められた D E S 方式と同じブロック暗号方式である。さらに、この顧客視聴許可システム 3 は、顧客管理システム 2 から供

給された EMM データに含まれているワークキー K_w を、暗号化アルゴリズム C R Y P S によって暗号化されたワークキー K_w' に置換え、新たな暗号化された EMM データを生成する。また、顧客視聴許可システム 3 は、この当社独自の暗号アルゴリズムによって暗号化された EMM データを衛星を介して伝送するためには、この暗号化された EMM データをトランスポートストリームパケットのペイロード部に挿入することによって、暗号化された EMM データをトランスポートストリームパケットの形態に変換する。以下の説明において、この EMM データを含んだトランスポートストリームパケットを EMM パケットと呼ぶ。尚、この顧客視聴許可システム 3 は、この EMM パケットに付与される P I D (パケット識別子) を、後述するエンコーダ／マルチプレクサコントロールユニット 9 からネットワークを介して受け取る。

さらに、この顧客視聴許可システム 3 は、256 個のワークキー (K_w) とそのワークキーを識別するためのワークキー識別番号 ($K_w _ N_0$) とを対応付けたワークキーテーブルを有しており、このワークキーテーブルをネットワークを介してマルチプレクサシステム 8 内のメモリにダウンロードする。このようなワークキーテーブルをマルチプレクサシステム 8 にダウンロードする理由は、この視聴許可システム 3 からマルチプレクサシステム 8 には暗号化されたワークキー K_w' しか伝送されないので、マルチプレクサシステム 8 においてワークキー識別番号 ($K_w _ N_0$) から暗号化されていないワークキー K_w を得るためである。

また、この顧客視聴許可システム 3 は、伝送されるプログラムに含まれる各データエレメントにスクランブルを施すためのスクランブルキー K_s を生成する。顧客視聴許可システム 3 は、各プログラム毎又はプログラムに含まれる各データエレメント毎に異なるスクランブルキー K_s を生成する。例えば、図 2 に示すように、第 1 のプログラムを構成するビデオデータ及びメインオーディオデータをそれぞれスクランブルするためのスクランブルキーとして $K_s 1$ を生成し、第 2 のプログラムのビデオデータ及びメインオーディオデータをスクランブルするた

めのスクランブルキーとしてKs2を生成し、第2のプログラムのサブオーディオデータをスクランブルするためのスクランブルキーとしてKs3を生成し、第2のプログラムのプライベートデータをスクランブルするためのスクランブルキーとしてKs4を生成する。どのプログラムのどのエレメントに対してどのようなスクランブルキーを割り当てるかは、プログラム内容に応じて顧客視聴許可システム3が自由に決定できる。例えば、第4のプログラムのように、ビデオデータ、メインオーディオデータ、サブオーディオデータ及びプライベートデータに対してそれぞれ異なるスクランブルキーKs7～Ks10を設定したり、又は、第5のプログラムのように、ビデオデータ、メインオーディオデータ、サブオーディオデータ及びプライベートデータに対してそれぞれ同じスクランブルキーKs11を設定したりするような自由な設定が可能である。

さらに、顧客視聴許可システム3は、このデジタル放送システムにおける暗号／暗号解読システムのセキュリティを高めるため、顧客視聴許可システム3の内部に設けられた乱数発生器によって、これらのスクランブルキーKs1～Ks19を4秒おきに更新している。

また、顧客視聴許可システム3は、スクランブルを解除するために使用される複数のECM (Entitlement_Control_Message) データを生成する。このECMデータは、ワークキーテーブルの中の少なくとも1つのワークキーKwを指定するためのワークキー番号、及びデータストリームに対してスクランブルをかけるためのスクランブルキーKs、及び、この顧客視聴許可システム3を識別するためのCA_system_ID等のデータから構成されている。従って、1つのECMデータには、1つのスクランブルキーしか登録できないので、図2に示した19個のスクランブルキーKs1～Ks19を使用する例においては、顧客視聴許可システム3は、19個のECMデータを生成する。

さらに、顧客視聴許可システム3は、生成された複数のECMデータを伝送するために、この複数のECMデータをトランSPORTストリームパケットのペイ

ロード部に挿入することによって、複数のECMデータをトランSPORTストリームパケットの形態にそれぞれ変換する。以下の説明において、このECMデータを含んだトランSPORTストリームパケットをECMパケットとして説明する。また、図1においては、スクランブルキーKs1を含んだECMパケットをECM1と記し、スクランブルキーKs2を含んだECMパケットをECM2と記し、以下同様にして、スクランブルキーKs3～Ks19を含んだECMパケットをそれぞれECM3～ECM19と記している。尚、この顧客視聴許可システム3は、この複数のECMパケットに付与されるPID(パケット識別子)を、後述するエンコーダ/マルチプレクサコントロールユニット9からネットワークを介して受け取る。また、図1には、ECMパケットが、直接マルチプレクサシステムに供給されるように記されているが、これはECMパケットの送出元及び送り先をわかりやすく示すためだけであって、実際には、ネットワーク及びエンコーダ/マルチプレクサコントロールユニット9を介してマルチプレクサシステム8に供給される。

次に、デジタル放送システムにおいて上述したワークキー及びスクランブルキーを使用する理由について説明する。

一般的なデジタル放送システムにおいては、番組視聴契約を行った特定の視聴者のみに視聴を許可すると共に、番組の契約内容に応じてその特定の視聴者に課金する有料放送システムが適用されている。このデジタル放送システムにおいて有料放送システムを実現するためには、放送局側で作成したスクランブルキーを使用して伝送すべきプログラムにスクランブルをかけ、番組視聴契約を行った特定視聴者のみがそのスクランブルを解除してプログラムを視聴できるようにしなければいけない。スクランブルが施されたデータエレメントを受信機側において特定視聴者のみが解読できるようにするためには、スクランブルする際に使用したスクランブルキーKsを使用することによってスクランブルを解除する必要がある。衛星を介して伝送されたプログラムのスクランブルを自動で解除するためには、このスクランブルキーKsを受信機側に伝送しなければいけない。

しかしながら、このスクランブルキーK_sを受信機側に伝送してしまうと、番組契約していない視聴者がこのスクランブルキーK_sを取得し、その結果伝送された全てのプログラムを無料で視聴できることになってしまう。よって、本発明の有料放送システムでは、第1のセキュリティとして、このスクランブルキーK_sを、乱数発生器を使用して数秒単位で変更するとともに、ワークキーK_wによって、このスクランブルキーK_sを暗号化している。この乱数発生器を使用したスクランブルキーK_sの暗号化は、ソフトウェアによって実現できるので、暗号強度としてはかなりセキュリティが高いといえる。

本発明のデジタル放送システムでは、さらに一層、限定受信システムのセキュリティを高めるために、このスクランブルキーK_sを、マルチプレクサシステム8の後述する暗号化回路822においてワークキーK_wを使用して暗号化し、暗号化したスクランブルキーK_{s'}を受信機側に伝送するようにしている。つまり、プログラムのスクランブルに使用したスクランブルキーK_sをそのまま送るのでは無く、そのスクランブルキーK_s自体を暗号化して送ることによって、セキュリティを最大限にまで高めている。また、受信機側において、この暗号化されたスクランブルキーK_{s'}の暗号化を解くための解読器（Decrypter）は、受信機内のセキュリティモジュール（I Cカード）内に収められており、この暗号解読処理は全てこのセキュリティモジュール内部で行われる。このI Cカードから構成されるセキュリティモジュールは、内部のプログラムコードを解読することは事実上不可能な構造とされ、従って、全く異なる第3者がこのスクランブルキーの暗号を解くことは極めて困難であるといえる。

EPGシステム4は、伝送されたプログラムに関連する番組ガイドデータを作成するためのシステムである。番組ガイドデータ（EPGデータ）とは、例えば、今後の放送予定のプログラムの放送時間の案内データ、指定された番組の内容を説明するための文字データ、番組のタイトルデータ等のデータのことである。このEPGデータは、放送局が作成する場合が主であるが、プログラムをした番組供給会社が個別のEPGデータを作成する場合もあり得る。

サーバシステム 5 は、各種素材が記録されたディスクドライブをアレイ状に接続することによって構成されたサーバと、このサーバの記録／再生動作を制御するためのサーバ制御用コンピュータとから構成されている。このサーバシステム 5 は、放送番組編成システム 1 とイーサネット等の局内の LAN によって接続され、放送番組編成システムの番組編成リストに従ったプログラムを送出するよう制御される。このサーバシステム 5 に記録されている素材は、例えば、CM 素材を供給するための CM サーバ機能、テレビ番組素材やニュース番組素材を供給するためのデイリーサーバ機能、及び、テレビ番組素材や映画素材を供給するためのビデオオンデマンド (VOD) サーバ機能を有しており、放送番組編成システム 1 からの制御に基いて、任意のチャンネルに複数の任意のプログラムを出力することができる。

ルーティングシステム 6 は、サーバシステム 5 から供給された複数チャンネルのデータが適切なチャンネルから出力されるようにルーティングするためのシステムである。このルーティングシステム 6 は、放送番組編成システム 1 とイーサネットによって接続され、放送番組編成システムの番組編成リストに従ったプログラムを適切なチャンネルに送出するようにルーティング制御される。

エンコーダ／マルチプレクサコントロールユニット 9 は、エンコーディングシステム 7 及びマルチプレクサシステム 8 を制御するための制御コマンドを、ネットワークを介してエンコードシステム 7 及びマルチプレクサシステム 8 に供給する。エンコーダ／マルチプレクサコントロールユニット 9 は、EPG システム 4 からネットワークを介して EPG パケットを受け取ると共に、顧客視聴許可システム 3 からネットワークを介して ECM パケット (ECM1～ECM19) 及び EMM' パケットを受け取り、受け取った EPG パケット、EMM' パケット及び ECM パケットをマルチプレクサシステム 8 に供給する。さらに、エンコーダ／マルチプレクサコントロールユニット 9 は、エンコーディングシステム 7 にプライベートデータを供給すると共に、マルチプレクサシステム 8 にプログラム仕様情報 (PSI: Program_Specific_Information

) を供給する。

プログラム仕様情報 P S I は、指定されたプログラム番号とそのプログラム番号に対応するプログラムマップテーブル (P M T) のトランSPORTストリームパケットを指示するためのプログラムアソシエーションテーブル (P A T : Program_Association_Table) と、指定されたプログラムのデータエレメントが記述されたトランSPORTストリームパケットを指示するためのプログラムマップテーブル (P M T : Program_Map_Table) と、EMMデータが含まれるトランSPORTストリームパケットを指定するための条件付きアクセステーブル (C A T : Conditional_Access_Table) とから構成されている。エンコーダ／マルチプレクサコントロールユニット 9 は、プログラムアソシエーションテーブル P A T、プログラムマップテーブル P M T 及び条件付きアクセステーブル C A T を生成し、これらの生成したテーブルをトランSPORTストリームの形態で出力する。以下の説明において、プログラムアソシエーションテーブル P A T を含んだトランSPORTストリームパケットを P A T パケットと呼び、プログラムマップテーブル P M T を含んだトランSPORTストリームパケットを P M T パケットと呼び、条件付きアクセステーブル C A T を含んだトランSPORTストリームパケットを C A T パケットと呼ぶことにする。

また、エンコーダ／マルチプレクサコントロールユニット 9 は、E P G システム 4、顧客視聴許可システム 3 及びエンコーディングシステム 7 において作成したトランSPORTストリームパケットに対して適切なパケット識別子 P I D を設定するために、適切なパケット識別子 P I D を生成顧客視聴許可システム 3、E P G システム及びエンコーディングシステム 7 に供給する。

パケット識別子 (P I D : Packet_Identification) は、トランSPORTストリームパケットを識別するための識別子である。このパケット識別子 P I D は、トランSPORTストリームパケットのペイロード中に蓄積されるデータの種類に応じて決定される 13 ビットの固有のデータである。例え

ば、図 3 に示すように、ペイロード中にプログラムアソシエーションテーブル P A T に関する情報が蓄積されたトランSPORTストリームパケットの P I D 値として「0 x 0 0 0 0」が指定され、ペイロード中に条件付きアクセステーブル C A T に関する情報が蓄積されたトランSPORTストリームパケットの P I D 値として「0 x 0 0 0 1」が指定されている。また、ペイロード中にビデオデータやオーディオデータ等のエレメンタリーデータやプログラムマップテーブル P M T に関する情報が蓄積されたトランSPORTストリームパケットの P I D 値として、「0 x 0 0 2 0」～「0 x 1 F F E」の間の何れかの P I D 値が選択される。

また、エンコーダ／マルチプレクサコントロールユニット 9 は、各トランSPORTストリームパケットに対して設定される P I D を生成する際に、各トランSPORTストリームパケットに対して設定した P I D とスクランブル処理に使用するスクランブルキー K s とを対応付けた P I D テーブルを生成する。この P I D テーブルは、過去において使用した P I D 値を記憶しておくためのテーブルであって、このエンコーダ／マルチプレクサコントロールユニット 9 は、この P I D テーブルに記憶された P I D 値を参照することによって、過去において使用した P I D を認識し、過去の P I D と重複しないような新しい P I D 値を生成することができる。また、この P I D テーブルは、多重化されたトランSPORTストリームパケットをスクランブルするかしないかを決定する際に使用されるテーブルである。

例えば、P I D テーブルは、図 4 に示すように、生成されたトランSPORTストリームパケットに対して設定された P I D 値と、対応するトランSPORTストリームパケットに蓄積されているデータに対して設定されたスクランブルキーとを対応付けたテーブルである。この図 4 は、P A T パケットを示す P I D 値は、固定の「0 x 0 0 0 0」であって、第 1 のプログラムに対応する P M T パケットに対して設定された P I D 値は「0 x 0 1 0 0」であって、第 2 のプログラムに対応する P M T パケットに対して設定された P I D 値は「0 x 0 1 0 1」であって、第 1 のプログラムのビデオデータのパケットである V i d e o [1] パッ

ト及びメインオーディオデータのパケットであるMain_Audio [1] パケットをスクランブルするためのスクランブルキーKs1を有したECMパケットに対して設定されたPID値は「0x0300」であって、第2のプログラムのビデオデータのパケットであるVideo [2] パケットをスクランブルするためのスクランブルキーKs2を有したECMパケットに対して設定されたPID値は「0x0301」であって、第2のプログラムのメインオーディオデータのパケットであるMain_Audio [2] パケットをスクランブルするためのスクランブルキーKs2を有したECMパケットに対して設定されたPID値は「0x0302」であって、第2のプログラムのサブオーディオデータのパケットでSub_Audio [2] パケットをスクランブルするためのスクランブルキーKs3を含んだECMパケットに対して設定されたPID値は「0x0303」であって、第2のプログラムのプライベートデータのパケットであるPrivate [2] パケットをスクランブルするためのスクランブルキーKs4を含んだECMパケットに対して設定されたPID値は「0x0304」である。また、第1のプログラムのビデオデータのパケットであるVideo [1] に対して設定されたPID値は「0x0500」であって、このパケットはスクランブルキーKs1を用いてスクランブルがかけられ、第1のプログラムのメインオーディオデータのパケットであるMain_Audio [1] パケットに対して設定されたPID値は「0x0501」であって、このパケットはスクランブルキーKs1を用いてスクランブルがかけられ、第2のプログラムのビデオデータのパケットであるVideo [2] パケットに対して設定されたPID値は「0x0502」であって、このパケットはスクランブルキーKs2を用いてスクランブルがかけられる。またCATパケットを示すPID値は固定の「0x0001」であって、EMMパケットに対して設定されたPID値は「0x700」である。

エンコーディングシステム7は、図5に示されるように、MPEG2規格に基いて供給された複数チャンネルのビデオデータをエンコードするための複数のM

PEGビデオエンコーダ711V～719Vと、ビデオデータにそれぞれ対応する複数のオーディオデータをMPEG2規格に基いて符号化するためのMPEGオーディオエンコーダ711A方719Aと、各ビデオエンコーダ、各オーディオエンコーダからのストリーム及びエンコーダ／マルチプレクサコントロールユニット9から供給されたプライベートデータストリームを多重化するための多重化回路721～729と、各ビデオ／オーディオエンコーダ711～719及び多重化回路721～719をそれぞれ制御するためのエンコーディングコントローラ70とを有している。この図5に示されるエンコーディングシステムは、9チャンネルのプログラムをエンコードする構成となっているが、9チャンネルに限らず何チャンネルであっても良いことは言うまでもない。

各ビデオエンコーダ711V～719Vは、ビデオデータをMPEG2規格に基いてエンコードすることによって符号化ビットストリームを生成する。続いて、各ビデオエンコーダは、このビットストリームを1ピクチャ単位で分割すると共にその分割されたビットストリームにヘッダを付加することによってPES(Packetized Elementary Stream)パケットを生成する。そして、さらに各ビデオエンコーダは、PESパケットを184バイト単位に分割し、その分割された184バイトのビットストリームに4バイトのヘッダを付与することによって、トランSPORTストリームパケットを生成する。トランSPORTストリームパケットが連続してストリーム状になっているデータのことをトランSPORTストリームと呼んでいる。また、トランSPORTストリームパケットを生成する際に、エンコーダ／マルチプレクサコントロールユニット9から、各ビデオエンコーダ711V～719Vに対して、この符号化されたビデオデータを含んだトランSPORTストリームパケットを識別するためのパケット識別子(PID)がそれぞれ供給される。

また、各オーディオエンコーダ711A～719Aは、メインオーディオデータやサブオーディオデータをMPEG2規格に基いてエンコードすることによって符号化されたビットストリームを生成する。ビデオエンコーダと同じように、

各オーディオエンコーダ 711A～719A は、このビットストリームから PES パケットを生成し、この PES パケットを 184 バイト単位に分割し、4 バイトのヘッダを付与することによってオーディオデータを含んだトランSPORTストリームパケットを生成する。また、トランSPORTストリームパケットを生成する際に、エンコーダ／マルチプレクサコントロールユニット 9 から、各オーディオエンコーダ 711A～719A に対して、この符号化されたオーディオデータを含んだトランSPORTストリームパケットを識別するためのパケット識別子 (PID) がそれぞれ供給される。

多重化回路 721～729 は、符号化ビデオデータを含んだトランSPORTストリーム、符号化オーディオデータを含んだトランSPORTストリーム及びプライベートデータを含んだトランSPORTストリームを多重化して、1 つのトランSPORTストリームを生成する。具体的には、多重化回路は、符号化ビデオデータを含んだトランSPORTストリーム、符号化オーディオデータを含んだトランSPORTストリーム及びプライベートデータを含んだトランSPORTストリームを、トランSPORTストリームパケット単位で切換えることによって、これらのストリームを多重化する。従って、出力されるトランSPORTストリーム中には、符号化ビデオデータを含んだトランSPORTストリームパケットと、符号化オーディオデータを含んだトランSPORTストリームパケットと、プライベートデータを含んだトランSPORTストリームパケットが混在している。因みに、プライベートデータはエンコーディングコントローラ 70 によってトランSPORTストリームパケット化されてネットワークを介して各多重化回路に供給される。

エンコーディングコントローラ 70 は、各ビデオエンコーダ及びオーディオエンコーダに対して、適切な符号化ビットレートを指定する。例えば、エンコーディングコントローラ 70 は、スポーツ等の符号化ビット量を多く必要とするプログラムをエンコードするためのエンコーダには、高いビットレートを割当て、ニュース映像などの比較的、符号化時の発生ビット量が少ないとと思われるプログラムをエンコードするエンコーダに対しては、低いビットレートを割り当てる。つ

まり、各チャンネルのビデオデータの複雑度（符号化する際にどれだけビット量が発生するかを示す指標として用いられている）を相対的に把握し、複雑度が高いビデオデータのチャンネルから順に高いビットレートを割り当てるようしている。もちろん、割当てられたビットレートはプログラム固有では無くて、プログラム内のビデオデータの複雑度に応じてその都度変更される。

次に、このトランSPORTストリームパケットの構造及びトランSPORTストリームパケットのシンタックスについて、図6から図9を参照して詳しく説明する。

トランSPORTストリームパケットは、4バイトのヘッダと、各種のデータ及びデータエレメントを格納するための184バイトのペーロード部とから構成されている。

トランSPORTストリームパケットのヘッダ部は、sync_byte、transport_error_indicator、payload_unit_start_indicator、transport_priority_、PID、transport_scrambling_control、adaptation_field_control、continuity_counter、及びadaptation_field等の各種フィールドから構成されている。

sync_byteとは、ビットストリーム中から同期パターンを検出するための固定の8ビットのフィールドである。値は‘01000111’(0X47)の固定値で定義され、このストリーム中のこのビットパターンを検出することによって、同期を検出することができる。

transport_error_indicatorは、1ビットのフラグである、「1」に設定されると、少なくとも1ビットの訂正できないビットエラーがトランSPORTストリームパケットに存在することを示す。

payload_unit_start_indicatorは、1ビットのフラグである。ビデオ／オーディオデータ等のエレメンタリーデータまたはプロ

グラム仕様情報 (P S I) を伝送するトランSPORTストリームパケットに対して規範的な意味を有するデータである。トランSPORTストリームパケットのペイロードがエレメンタリーデータを含む場合、payload_unit_start_indicatorは、次の意味を有する。payload_unit_start_indicatorが「1」の場合には、このトランSPORTストリームパケットのペイロードの最初に、エレメンタリーデータが挿入されていることを示し、payload_unit_start_indicatorが「0」の場合には、このトランSPORTストリームパケットのペイロードの最初に、エレメンタリーデータが挿入されていないことを示す。もし、payload_unit_start_indicatorが「1」にセットされると、ただ一つのPESパケットが任意のトランSPORTストリームパケットで開始することを示す。一方、トランSPORTストリームパケットのペイロードがP S Iデータを含む場合、payload_unit_start_indicatorは、次の意味を有する。もし、トランSPORTパケットがP S Iセクションの第1バイトを伝送する場合、payload_unit_start_indicatorは「1」となる。もし、トランSPORTストリームパケットがP S Iセクションの第1バイトを伝送していない場合、payload_unit_start_indicatorは「0」となる。尚、トランSPORTストリームパケットがヌルパケットの場合にも、payload_unit_start_indicatorは「0」となる。

transport_priorityは、トランSPORTパケットの優先度を示す1ビットの識別子である。このtransport_priorityが「1」に設定されると、このトランSPORTパケットは、同一のパケット識別子P I Dをもつパケットであって、このtransport_priorityが「1」でないパケットより優先度が高いことを示している。例えば、このtransport_priorityのパケット識別子を設定することによって、一つのエレメンタリーストリーム内において任意のパケットに優先度をつけること

ができる。

`transport_scrambling_control` は、トランSPORTストリームパケットペイロードのスクランブリングモードを示す2ビットのデータである。スクランブリングモードとは、ペイロードに格納されたデータがスクランブルされているか否か及びそのスクランブルの種類を示すためのモードである。トランSPORTストリームパケットヘッダ、およびアダプテーションフィールドは、スクランブルキーKsによってスクランブルされなければならないように規格化されている。よって、この`transport_scrambling_control`によって、トランSPORTストリームパケットペイロードに格納されたデータがスクランブルされているか否かを判断することができる。

`adaptation_field_control` は、このトランSPORTストリームのパケットヘッダにアダプテーションフィールド及び／又はペイロードがくることを示す2ビットのデータである。具体的には、パケットヘッダにペイロードデータのみが配置される場合には、この`adaptation_field_control`は「01」となり、パケットヘッダにアダプテーションフィールドのみが配置される場合には、この`adaptation_field_control`は「10」となり、パケットヘッダにアダプテーションフィールドとペイロードとが配置される場合には、この`adaptation_field_control`は「11」となる。

`continuity_counter` は、連続して伝送された同じP I Dをもつパケットが、伝送途中で一部欠落又は捨てられか否かを示すためのデータである。具体的には、`continuity_counter` は、同一のP I Dを有する各トランSPORTストリームパケットごとに増加する4ビットのフィールドである。但し、この`continuity_counter` がカウントされるときは、パケットヘッダにアダムテーションフィールドが配置されている場合である。

`adaptation_field` は、個別ストリームに関する付加情報やス

タッフィングバイト等をオプションとして挿入するためのフィールドである。このアダプテーションフィールドによって、個別ストリームの動的な状態変化に関するあらゆる情報をデータと一緒に伝送することができる。

`adaptation_field`は、`adaptation_field_length`、`discontinuity_counter`、`random_access_indicator`、`elementary_stream_priority_indicator`、`OPCR_flag`、`splicing_point_flag`、`splicing_point`、`transport_private_data_flag`、`adaptation_field_extension_flag`、`program_clock_reference (PCR)`、`original_program_clock_reference (OPCR)`、`sprice_countdown`、`transport_private_data_length`、`private_data`、`adaptation_field_extension_length`、`ltw_flag (legal_time_window_flag)`、`piece_wise_rate_flag`、及び`Seamless_splice_flag`等の各種フィールドから構成されている。

`adaptation_field_length`は、この`adaptation_field_length`の次に続くアダプテーションフィールドのバイト数を示すデータである。`adaptation_field_control`が「11」の場合には、`adaptation_field_length`は0から182ビットであって、`adaptation_field_control`が「10」の場合には、`adaptation_field_length`は183ビットとなる。尚、トランSPORTストリームのペイロードを満たすだけのエレメンタリーストリームが無い場合には、ビットを満たすためのスタッフィング処理が必要となる。

`discontinuity_counter` は、同じ P I D を有する複数のパケットの途中において、システムクロックリファレンス (S C R) がリセットされ、システムクロックリファレンスが不連続になっているか否かを示すデータである。もし、システムクロックリファレンスが不連続の場合には、この `discontinuity_counter` は「1」となり、システムクロックリファレンスが連続している場合には、この `discontinuity_counter` は「0」となる。尚、このシステムクロックリファレンスとは、ビデオ及びオーディオのデコードするための M P E G デコーダにおいて、デコーダ側のシステムタイムロックの値をエンコーダ側において意図したタイミングに設定するための参照情報である。

`random_access_indicator` は、ビデオのシーケンスヘッダ又はオーディオのフレームの始まりを示すデータである。つまり、この `random_access_indicator` は、データエレメントのランダムアクセスを行うときに、ビデオ又はオーディオのアクセスポイント（フレームの始まりのこと）であることを示すためのデータである。

`elementary_stream_priority_indicator` は、同一の P I D を有するパケットにおいて、このトランSPORTストリームパケットのペイロード中で伝送されるエレメンタリーストリームデータの優先度を示すデータである。例えば、エレメンタリーストリームのビデオデータが、そのビデオデータがイントラ符号化されている場合に、`elementary_stream_priority_indicator` が「1」にセットされる。それに対して、インター符号化されているビデオデータを含んだトランSPORTストリームの `elementary_stream_priority_indicator` は、「0」にセットされる。

`PCR_flag` は、アダプテーションフィールド内に P C R (p r o - g r a m _ c l o c k _ r e f e r e n c e) データが存在するか否かを示すデータである。アダプテーションフィールド内に P C R データが存在する場合には、P

CR_flagが「1」にセットされ、PCRデータが存在しない場合には、PCR_flagが「0」にセットされる。尚、このPCRデータとは、受信機側のデコーダにおいて、伝送されたデータをデコードするデコード処理のタイミングを得るために使用されるデータである。

OPCR_flagは、アダプテーションフィールド内にOPCR(original_program_clock_reference)データが存在するか否かを示すデータである。アダプテーションフィールド内にOPCRデータが存在する場合には、OPCR_flagが「1」にセットされ、OPCRデータが存在しない場合には、OPCR_flagが「0」にセットされる。このOPCRデータとは、スライシング処理等によって、複数のオリジナルトランSPORTストリームから1つのトランSPORTストリームを再構築したときのに使用されるデータであって、あるオリジナルトランSPORTストリームのPCRデータを表わすデータである。

splicing_point_flagは、トランSPORTレベルでの編集ポイント(スライスポイント)を示すためのsplice_count-downがアダプテーションフィールド内に存在するか否かを示すデータである。アダプテーションフィールド内に^splice_countdownが存在する場合には、このsplicing_point_flagは「1」であって、アダプテーションフィールド内にsplice_countdownが存在する場合には、このsplicing_point_flagは「0」である。

transport_private_data_flagは、アダプテーションフィールド内に、任意のユーザデータを記述するためのプライベートが存在するか否かを示すためのデータである。アダプテーションフィールド内にプライベートが存在する場合には、このtransport_private_data_flag「1」にセットされ、アダプテーションフィールド内にプライベートが存在しない場合には、このtransport_private_data_flagは「0」にセットされる。

`adaptation_field_extension_flag` は、アダプテーションフィールド内に、拡張フィールド存在するか否かを示すためのデータである。アダプテーションフィールド内に拡張フィールドが存在する場合には、この `adaptation_field_extension_flag` は「1」にセットされ、アダプテーションフィールド内に拡張フィールドが存在しない場合には、この `adaptation_field_extension_flag` は「0」にセットされる。

`program_clock_reference` (PCR) は、送信側とクロックの位相に対して受信機側のクロックの位相を同期させるときに参照する基準クロックである。この PCR データには、トランスポートパケットが生成された時間が格納されている。この PCR は、33ビットの `program_clock_reference_base` と 9ビットの `program_clock_reference_extension` との 42ビットから構成されるデータである。`program_clock_reference_extension` によって 0 ~ 299までのシステムクロックをカウントし、299から 0 にリセットされる際のキャリーによって、`program_clock_reference_base` に 1ビットを加算することによって、24時間をカウントすることができる。

`original_program_clock_reference` (IO PCR) は、あるトランスポートストリームから単一プログラムのトランスポートストリームを再構成するときに使用されるデータである。単一プログラムドラムストリームが完全に再構成された場合、この `original_program_clock_reference` は `program_clock_reference` にコピーされる。

`splice_countdown` は、同一 PID のトランスポートストリームパケットにおいて、トランスポートストリームパケットレベルで編集可能（スプライシング処理可能）なポイントまでのパケットの数を示すデータである。従

って、編集可能なスプライシングポイントのトランSPORTストリームパケットでは、`splice_countdown`は「0」である。`splice_countdown`が「0」になるトランSPORTパケットで、トランSPORTストリームパケットペイロードの最終バイトは、符号化されたピクチャの最後のバイト.とすることによって、スプライシング処理が可能となる。

このスプライシング処理とは、トランSPORTレベルで行われる2つの異なるエレメンタリーストリームを連結し、1つの新しいトランSPORTストリームを生成する処理のことである。そして、スプライシング処理として、復号の不連続性を発生しないシームレススプライスと、復号の不連続性を引き起こすノンシームレススプライスとに分けることができる。符号の不連続性を発生しないとは、新しく後ろにつなげられたストリームのアクセスユニットの復号時間と、スプライス前の古いストリームのアクセスユニットの復号時間と間の矛盾が無いことを示し、符号の不連続性を発生するとは、新しく後ろにつなげられたストリームのアクセスユニットの復号時間に対して、スプライス前の古いストリームのアクセスユニットの復号時間の矛盾が生じることを示している。

`transport_private_data_length`は、アダプテーションフィールドにおけるプライデータデータのバイト数を示すデータである。

`private_data`は、規格では特に規定されておらず、アダプテーションフィールドにおいて任意のユーザデータを記述することができるフィールドである。

`adaptation_field_extension_length`は、アダプテーションフィールドにおけるアダプテーションフィールドエクステンションのデータ長を示すデータである。

`ltw_flag (legal_time_window_flag)`は、アダプテーションフィールドにおいて表示ウインドウのオフセット値を示す`ltw_offset`が存在するか否かを示すデータである。

`piecewise_rate_flag` は、アダプテーションフィールドにおいて `piecewise_rate` が存在するか否かを示すデータである。

`seamless_splice_flag` は、スプライシングポイントが、通常のスプライシングポイントか、シームレススプライシングポイントであるかを示すデータである。この `seamless_splice_flag` が「0」の時は、スプライシングポイントが通常のスプライシングポイントであることを示し、この `seamless_splice_flag` が「1」の時は、スプライシングポイントがシームレススプライシングポイントであることを示している。通常のスプライシングポイントとは、スプライシングポイントが PES パケットの区切りに存在する場合であって、このスプライシングポイントの直前のスプライシングパケットがアクセスユニットで終了し、次の同じ PID を有するトランスポートパケットが PES パケットのヘッダで開始している場合である。これに對して、シームレススプライシングポイントとは、PES パケットの途中にスプライシングポイントがある場合であって、新しく後ろにつなげられたストリームのアクセスユニットの復号時間と、スライス前の古いストリームのアクセスユニットの復号時間との間に矛盾が無いようにするために、古いストリームの特性の一部を、新しいストリームの特性として使う場合である。

次に、図 10 を参考してマルチプレクサシステム 8 について詳細に説明する。このマルチプレクサシステム 8 は、PAT パケット、PMT パケット、CAT パケット、符号化されたエレメンタリデータを含んだトランSPORTストリームパケット、EPG パケット、ECM パケット、及び EMM. パケットを多重化し、1 つのトランSPORTストリームを生成するためのシステムである。

具体的には、このマルチプレクサシステム 8 は、このマルチプレクサシステム 8 内の全ての回路を管理するマルチプレクサコントローラ 81 と、顧客視聴許可システム 3 から供給された ECM パケットを暗号化するための暗号化ブロック 82 と、エンコーダ/マルチプレクサシステム 9 からプログラム仕様情報 PSI として供給された PAT パケット、PMT パケット及び CAT パケットをそれぞれ

バッファリングするための FIFO バッファ 841～843、複数のプログラムを含んだトランSPORTストリームパケットをそれぞれバッファリングするための FIFO バッファ 851～859、ECM パケット、EMM パケット及び EP G パケットをそれぞれバッファリングするための FIFO バッファ 861～863、各 FIFO バッファのリード／ライトを制御すると共に、各 FIFO バッファの空き容量を監視する FIFO コントローラ 83 と、各 FIFO バッファから出力されたトランSPORTストリームパケットを多重化して多重化されたトランSPORTストリームを生成する多重化回路 87 と、多重化されたトランSPORTストリームパケットに含まれるデータエレメントにスクランブルを施すスクランブルブロック 88 とを備えている。

マルチプレクサコントローラ 81 は、エンコーダ／マルチプレクサコントロールユニット 9 から EP G パケット、EMM' パケット、ECM パケット (ECM 1～ECM 19) 、PAT パケット、PMT パケット及び CAT パケットを受取り、各パケットを適切な回路に供給する。また、マルチプレクサコントローラ 81 は、エンコーダ／マルチプレクサコントロールユニット 9 から PID テーブルを受取り、この PID テーブルをスクランブルブロック 88 に供給する。

暗号化ブロック 82 は、エンコーダ／マルチプレクサコントロールユニット 9 及びマルチプレクサコントローラ 81 を介して顧客視聴許可システム 3 から供給された複数の ECM パケットに含まれるスクランブルキー Ks を暗号化 (En-crypt) するためのブロックである。暗号化ブロック 82 は、顧客視聴許可システム 3 からダウンロードされたワークキーテーブルを暗号化処理の前に予め記憶しておくための RAM 821 と、ワークキー Kw に基いて ECM に含まれるスクランブルキー Ks を暗号化する暗号化回路 (Encrypter) 822 を有している。

次に、この暗号化ブロック 82 における暗号化処理の動作を、第 1 のプログラムを構成するエレメンタリーデータをスクランブルするためのスクランブルキー Ks1 を暗号化する場合を例にあげて説明する。まず、ECM パケット ECM 1

に含まれるワークキー番号Kw_Noが、RAM821に供給される。RAM821には、顧客視聴許可システムからダウンロードされたワークキー番号Kw_NoとワークキーKwとを対応付けたワークキーテーブルが記憶されている。従って、RAM821にはECM1に含まれていたワークキー番号Kw_Noが供給されるので、供給されたワークキー番号Kw_Noに対応したワークキーKwがこのRAM821から出力される。暗号化回路822は、スクランブルキーKs1を含んだECMパケットを受け取ると共に、ワークキーKwをRAM821から受け取る。この暗号化回路822は、このワークキーKwを使用して、ソースECMに含まれているスクランブルキーKs1を暗号化し、暗号化されたスクランブルキーKs'を生成する。暗号化回路822は、ソースECMの暗号化されていないスクランブルキーKsの代わりに暗号化されたスクランブルキーKs'を蓄積し、この暗号化スクランブルキーKs'を含んだトランスポートストリームパケットを、暗号化ECMパケットとして出力する。尚、この暗号化アルゴリズムは、顧客視聴許可システム3において、EMMデータに含まれるワークキーKwを暗号化したときの暗号化アルゴリズムCRYSPと同じアルゴリズムである。

一方、この暗号化ブロック82は、ECMデータとして供給されたスクランブルキーKs1を、スクランブルブロック88に供給する。尚、このスクランブルブロック88に供給されるスクランブルキーKs1は、ワークキーKwによって暗号化されていないキーである。

第1のECMパケットECMに蓄積されているスクランブルキーKs1を暗号化する例について説明したが、他のスクランブルキーKs2～Ks19を暗号化する処理も全く同じである。よって、暗号化ブロック82からは、暗号化ECMパケットECM1'～ECM19'が出力されてFIFOバッファ861に供給されると共に、暗号化ブロック82からは、暗号化されていないスクランブルキーKs1～Ks19が出力されてスクランブルブロック88に供給される。

多重化回路87は、FIFO841～843にバッファリングされたPATパ

ケット、PMTパケット又はCATパケット、FIFO851～859にバッファリングされた複数のプログラムProgram1～Program9をそれぞれ含んだ各トランSPORTストリームパケット、FIFO861～863にバッファリングされたECMパケット、EMMパケット又はEPGパケットのいずれかを、各FIFOのデータ量に応じて選択しながらスクランブルブロック88に供給する。このとき、FIFOコントローラ83は各FIFOに入力されるパケットデータの入力レートを監視しており、各FIFOごとの入力レートの総和が所定の出力レートを越えているとき、この過入力レートの状態をマルチプレクサコントローラ81に供給する。この結果、マルチプレクサコントローラ81は、多重化回路87によって選択される選択対象としての各FIFOのうち、EMMパケットをバッファリングするFIFO862を選択対象外に除外し、残りのFIFOを選択対象として切り換えながら、その切り換えられたFIFOのパケットデータをスクランブルブロック88に供給する。この結果、多重化回路87は選択すべきFIFOの数が少なくなることにより、選択対象であるFIFOの選択回数が増加し、これにより過入力レート状態に対応して各FIFOのデータ出力レートを増加させることができる。

そして、各FIFOごとの入力レートの総和が所定の出力レートを下回ったとき、マルチプレクサコントローラ81はFIFO862を多重化回路87の選択対象に復帰させることにより、FIFO862にバッファリングされているEMMパケットをスクランブルブロック88に供給する。この場合、FIFO862にバッファリングされている視聴者の契約内容を表すEMMデータは、そのデータ内容が頻繁に変更されることはなく、多重化回路87による選択対象から一時的に除外されても、実用上不都合を生じさせることはない。

また、各FIFOごとの入力レートの総和がさらに増加して、1つのFIFO862を多重化回路87の選択対象外に除外するだけでは過入力レート状態に対応しきれなくなると、マルチプレクサコントローラ81は、EMMデータをバッファリングしているFIFO862に加えて、EPGデータをバッファリングし

ている FIFO 8 6 3 を選択対象外に除外する。これにより、多重化回路 8 7 によつて選択される FIFO の数がさらに少なくなり、選択対象である FIFO の選択回数がさらに増加し、これによりこのときの過入力レート状態に対応して各 FIFO のデータ出力レートをさらに増加することができる。この場合、FIFO 8 6 3 にバッファリングされている番組ガイド情報である EPG データは、そのデータ内容が頻繁に変更されることはなく、多重化回路 8 7 による選択対象から一時的に除外されても、実用上不都合を生じさせることはない。

スクランブルブロック 8 8 は、PID 検出回路 8 8 1 と、スクランブル回路 8 8 2 とを有している。PID 検出回路 8 8 1 は、多重化回路 8 7 から出力されたトランSPORTストリームパケットを受け取ると共に、エンコーダ／マルチプレクサコントロールユニット 9 からマルチプレクサコントローラ 8 1 を介して PID テーブル（図 4）を受け取る。この PID テーブルには、トランSPORTストリームを生成する際に使用した PID 値とスクランブルキーとが対応付けられて記憶されているので、PID 検出回路 8 8 1 は PID テーブルに登録された PID 値を参照することによって、使用するスクランブルキー Ks を検索し、その検索されたスクランブルキー Ks をスクランブル回路 8 8 2 に供給する。スクランブル回路 8 8 2 は、PID 検出回路 8 8 1 から供給されたスクランブルキー Ks を用いて、このスクランブルキー Ks に対応付けられたプログラムデータを含むトランSPORTストリームパケットにスクランブルをかけ、変調回路 1 0 （図 1）に出力する。

次にプログラム仕様情報について説明する。

プログラム仕様情報（PSI：Program_Specific_Information）とは、複数プログラム及びデータが多重化されたトランSPORTストリームパケットのどのパケットにどのようなデータが含まれているのかを示す情報である。従って、復号器はこのプログラム仕様情報を参照することによって、所望のデータをデコードすることができる。

このプログラム仕様情報は、図 1 1 に示す 4 つのテーブル構造に分類すること

ができる。プログラムアソシエーションテーブル（P A T : P r o g r a m _ A s s o c i a t i o n _ T a b l e ）は、指定されたプログラム番号とそのプログラム番号に対応するプログラムマップテーブル（P M T ）のP I Dを指示するためのテーブルである。プログラムマップテーブル（P M T : P r o g r a m _ M a p _ T a b l e ）は、指定されたプログラムのエレメントが記述されたパケットのP I Dを指示するためのテーブルである。網情報テーブル（N I T : N e t w o r k _ I n f o r m a t i o n _ T a b l e ）は、ネットワークに関するパタメータを伝送する際に仕様する情報であるが、規格では特に規定されていないプライベートなテーブルである。条件付きアクセステーブル（C A T : C o n d i t i o n a l _ A c c e s s _ T a b l e ）は、EMMパケットに固有のP I Dを割り当てるためのテーブルである。以下に、プログラムアソシエーションテーブル、プログラムマップテーブル及び条件付きアクセステーブルについて詳細に説明する。

まず、図1 2 及び図1 3 を参照して、プログラムアソシエーションテーブルに関して説明する。

プログラムアソシエーションテーブルP A Tは、伝送される各プログラムとそのプログラムの内容を指定しているトランSPORTストリームパケットのP I Dを指定するためのテーブルである。具体的には、このプログラムアソシエーションテーブルP A Tは、table_idとsection_syntax_indicatorと、section_lengthと、transport_stream_idと、version_numberと、current_next_indicatorと、section_numberと、last_section_numberと、program_numberと、network_P I Dと、program_map_P I Dとから構成されている。

table_idは、図1 4に示すように、各テーブルに対して割当てられた固有の識別番号である。プログラムアソシエーションテーブルP A Tのtable_idは「0 x 0 0」であって、条件付きアクセステーブルC A Tの

table_idは「0x01」であって、プログラムマップテーブルPMTのtable_idは「0x02」である。

section_syntax_indicatorは、「1」に固定された定数である。

section_lengthは、このsection_lengthの後のビットからCRCセクションの最後のバイトまでのバイト数を示すフィールドである。

transport_stream_idは、このトランSPORTストリームとネットワーク中に多重化されている他のトランSPORTストリームとを識別するための識別データである。

version_numberは、プログラムアソシエーションテーブル(PAT)のバージョン番号を示すデータである。このバージョン番号とは、プログラムアソシエーションテーブルの設定が変更されたときに、つまり、トランSPORTストリームの特性が変化する場合に1づつインクリメントされる0から31までの整数である。受信機側の復号器においては、このversion_numberを参照し、最も新しいバーションのセクションのみを有効と判断するようにしている。

current_next_indicatorは、伝送されているプログラムアソシエーションテーブルが現在使用可能であるか否かを示すデータである。

section_numberは、このプログラムアソシエーションテーブルセクションの番号を示すデータである。例えば、プログラムアソシエーションテーブルに含まれるprogram_association_section()のsection_numberは、最初のセクションであることを示すために、「0x00」に設定される。

last_section_numberは、このプログラムアソシエーションテーブルによって規定されている全てのセクションの中で最後のセクションのセクション番号を示すデータである。従って、このlast_section_

`number` によってプログラムアソシエーションテーブルによって規定されているセクション数を把握することができる。

`program_number` は、多重化される複数のプログラムに対して付与された固有の番号である。例えば、本発明のデータ伝送装置においては、多重化される 9 個のプログラムに対して、1 から 9 のプログラム番号が割当てられている。この `program_number` はユーザによって任意に定義することができるデータである。但し、この `program_number` が 0 にセットさせているときは、この `program_number` は、ストリーム中にネットワークインフォメーションテーブル (NIT) が存在していることを示す。

`network_PID` は、ストリーム中のネットワークインフォメーションテーブル (NIT) が記述されている PID を指し示すためのデータである。このネットワークインフォメーションテーブル (NIT) はユーザによって自由に設定することのできるテーブルであって、今回の装置においては使用されていない。

`program_map_pid` は、`program_number` で規定したプログラムに適用されるプログラムマップテーブルを有するトランSPORTストリームパケットの PID を示すデータである。例えば、あるプログラムが 1 つのビデオデータと 4 つのオーディオデータから構成されている場合には、このプログラムアソシエーションテーブル内に、そのあるプログラムのビデオデータを有するトランSPORTストリームパケットを指定する 1 つの PID と、そのあるプログラムのオーディオデータを有するトランSPORTストリームパケットを指定する 4 つの PID とが記述されている。

次に、図 15 及び図 16 を参照してプログラムマップテーブル (PMT) に関して説明する。

プログラムマップテーブルは、プログラム番号とそれらを構成するデータエレメント間のマッピングを与える。つまり、プログラムマップテーブルは、各プログラム番号毎に、そのプログラムを構成するビデオデータ、オーディオ及び付加

データ等のエレメントが伝送されるトランSPORTストリームパケットのP I Dを指定するためのセクションである。具体的には、このプログラムマップテーブルは、table_idと、section_syntax_indicatorと、section_lengthと、program_numberと、version_numberと、current_next_indicatorと、section_numberと、last_section_numberと、PCR_PIDと、program_info_lengthと、descriptor()と、stream_typeと、elementary_PIDと、ES_info_lengthと、descriptor()とから構成される。

table_idは、各テーブルを識別するために付与された固有の識別番号であって、プログラムマップテーブルのtable_idは「0 x 0 2」である。

section_syntax_indicatorは、「1」に固定された定数である。

section_lengthは、このsection_lengthの後のビットからCRCセクションの最後のバイトまでのバイト数を示すフィールドである。

program_numberは、多重化される複数のプログラムに対して付与された固有の番号である。例えば、本発明のデータ伝送装置においては、多重化される9個のプログラムに対して、1から9のプログラム番号が割当てられている。

version_numberは、プログラムマップテーブルを構成するためのプログラムマップセクションのバージョン番号を示すデータである。このバージョン番号は、プログラムマップセクションにおいて伝送されるデータが変更された場合に、バージョン番号がアップされる。

current_next_indicatorは、伝送されているプログラ

ムアソシエーションテーブルが現在使用可能であるか否かを示すデータである。プログラムアソシエーションテーブルが現在使用可能であれば、この current_next_indicator は「1」にセットされ、プログラムアソシエーションテーブルが現在使用可能でないならば、この current_next_indicator は「0」にセットされる。

section_number は、このプログラムマップテーブルに含まれているセクションの番号を示すデータであって、常に「0 x 00」にセットされている。なぜなら、このプログラムマップテーブルを構成するためにはプログラムマップセクションの1つしか存在しないからである。

last_section_number は、このプログラムマップテーブルによって規定されているセクションの中で最後のセクションのセクション番号を示すデータである。従って、プログラムマップテーブルを構成するためのプログラムマップセクションにおいては、この last_section_number は常に「0 x 00」にセットされている。

PCR_PID は、program_number で規定されるプログラムに対して有効である PCR データを含んでいるトランスポートパケットの PID を示すデータである。

program_info_length は、このフィールド program_info_length の次に記述されている descriptor () のバイト数を規定するためのデータである。

descriptor () は、プログラム及びプログラムエレメントの定義を拡張するために使用されるデータ構造である。例えば、ビデオエレメンタリーストリームの符号化パラメータを識別する基本的な情報を記述するための video_stream_descriptor () や、オーディオエレメンタリーストリームの符号化バージョンを識別する基本的な情報を記述するための Audio_stream_descriptor () や、複数のストリーム中に多重されている階層符号化されたビデオ及びオーディオを含むプログラムエ

レメント識別するための情報を記述する `hierarchy_descriptor()` や、プライベートデータを固有且つ明確に識別するための情報を記述する `re-registration_descriptor()` や、相互に関連するエレメンタリーストリーム中に存在するアライメントの種類を記述する `data_stream_alignment_descriptor()` や、伝送されたビデオデータの表示ウインドウの背景に表示されるバックグラウンドウインドウを指定するための情報を記述する `target_background_descriptor` や、伝送されたビデオデータの表示ウインドウの表示位置を指定するための情報を記述する `video_window_descriptor` や、受信契約情報EMMや番組解読情報ECM等のデータを記述するための `CA_descriptor()` や、言語及び関連するプログラムエレメントが使用する言語を識別するための情報が記述される `language_descriptor()` や、タイムスタンプの生成に使用されたシステムロックに関する情報を伝送するための `system_clock_descriptor()` や、 `video_buffer_verifier` を含む `STD(system_target_decoder)` 多重バッファにおけるデータ占有量のアンダーフロー及びオーバーフローの限界レベルを与えるためのデータを記述する `multiplex_buffer_utilization_descriptor()` や、オーディオ／ビジュアル作品の著作権を保護するために、それそれを識別を可能とするための情報を記述する `copyright_descriptor()` や、伝送されるデータエレメントの最大ビットレートを規定するための情報を記述する `maximum_bitrate_descriptor()` や、プライベータの伝送を規定するための `private_data_indicator_descriptor()` や、スムージングバッファのサイズ及びそのバッファから出力されるリークレートに関する情報を記述するための `smoothing_buffer_descriptor()` や、 `STD` バッファのリーク値を規定するための `STD_`

descriptor () や、符号化タイプに関する情報を記述するための i b p_descriptor () などの様々なディスクリプタから構成されている。

本発明のデータ伝送装置においては、このプログラムマップテーブルの中でこのdescriptor () が使用される場合には、このdescriptor () は、番組解読情報 ECM を含むトランSPORTストリームパケットの PID を指定するための情報を記述するために使用されている。

stream_type は、次の elementary_PID によって規定される PID を有するパケットに含まれるプログラムエレメントのタイプを規定するためのデータである。例えば、この stream_type は、パケットに含まれるプログラムエレメントが、ISO/IEC 11172 規格のビデオデータであれば「0x01」という値に設定され、ISO/IEC 13818-2 規格のビデオデータであれば、「0x02」という値に設定され、ISO/IEC 11172 規格のオーディオデータであれば「0x03」という値に設定され、ISO/IEC 13818-3 規格のオーディオデータであれば「0x04」という値に設定される。この stream_type は、このプログラムマップセクション中において、program_number で規定されたプログラムを構成するエレメントの数だけ繰返し記述されている。

elementary_PID は、program_number で規定されたプログラムを構成するエレメントを伝送するトランSPORTストリームパケットの PID を指定するためのフィールドである。この elementary_PID は、ストリームのエレメントのタイプを示す stream_type と対応付けられて記述されているデータである。

ES_info_length は、このフィールド ES_info_length の次に記述されているディスクリプタのバイト数を規定するためのデータである。

次に、図 17 及び図 18 を参照して、条件付きアクセステーブル (CAT) に

ついて詳細に説明する。この条件付きアクセステーブルは、有料放送において、ビデオデータやオーディオデータに対して施されたスクランブルを解除するためのに使用される受信契約情報EMMを伝送するパケットのPIDを規定するためのセクションである。また、この条件付きアクセステーブルは、受信契約者だけにプログラムのスクランブルが解除できるようにするための限定受信システム（CAシステム：Conditional Access System）と、受信契約情報EMMとの関係を規定するためのセクションでもある。

この条件付きアクセステーブルのPIDは、プログラムマップテーブルのようにプログラムアソシエーションテーブルによって指定されるのではなく、この条件付きアクセステーブルに対して割当てられた固有のPID値「0x01」をビットストリーム中から探し出すことによって、この条件付きアクセステーブルの各フィールドをデコードすることができる。

具体的には、この条件付きアクセステーブルは、table_idと、section_syntax_indicatorと、section_lengthと、version_numberと、current_next_indicatorと、section_numberと、last_section_numberと、descriptor()とから構成されている。

table_idは、各テーブルに対して割当てられた固有の識別番号であって、この条件付きアクセステーブルCATに割り当てられたtable_idは「0x01」である。は「0x02」である。

section_syntax_indicatorは、「1」に固定された定数である。section_lengthは、このsection_lengthの後のビットからCRCセクションの最後のバイトまでのバイト数を示すフィールドである。version_numberは、条件付きアクセステーブル（CAT）のバージョン番号を示すデータである。このversion_numberは、条件付きアクセステーブルの設定が変更されたとき

に、1づつインクリメントされる。current_next_indicatorは、伝送されている条件付きアクセステーブルが現在使用可能であるか否かを示すデータである。条件付きアクセステーブルが現在使用可能であれば、このcurrent_next_indicatorは「1」にセットされ、条件付きアクセステーブルが現在使用可能でないならば、このcurrent_next_indicatorは「0」にセットされる。

section_numberは、この条件付きアクセステーブルのセクション番号を示すデータである。例えば、条件付きアクセステーブルに含まれるCA_section()は、最初のセクションであることを示すために、「0x00」に設定される。この条件付きアクセステーブルに含まれるセクションが増える毎に、このsection_numberは1づつインクリメントされていく。

last_section_numberは、この条件付きアクセステーブルによって規定されている全てのセクションの中で最後のセクションのセクション番号を示すデータである。

descriptor()は、既に説明したように、プログラム及びプログラムエレメントの定義を拡張するために使用されるデータ構造である。本発明のデータ伝送装置においては、この条件付きアクセステーブルの中でこのdescriptor()が使用去れる場合には、このdescriptor()は、受信契約情報EMMを含むパケットのPIDを指定するための情報を記述するために使用されている。

次に、図19を参照して、プログラムマップテーブル及び条件付きアクセステーブル中で使用される条件付きアクセディスクリプタCA_descriptor()に関して説明する。

条件付きアクセディスクリプタは、受信契約に関する個人情報及び暗号化されたECMデータを解読するためのワークキーKwを含んだ受信契約情報EMMおよびビデオやオーディオ等のエレメンタリーストリームに対して施したスクラ

ンブルを解除するためのスクランブルキーKsを含んだ番組解読情報ECM等を規定するために使用される。従って、ビデオやオーディオ等のエレメンタリーストリームがスクランブルされている場合には、ビットストリーム中に、必ずこの条件付きアクセスディスクリプタが存在する。

条件付きアクセスディスクリプタCA_descriptor()は、descriptor_tag、descriptor_length、CA_system_ID、CA_PID、及びprivate_data_byteとから構成されるデータである。descriptor_tagは、すでに説明した複数のディスクリプタを識別するための固有の識別タグである。条件付きアクセスディスクリプタCA_descriptor()は、このdescriptor_tagとして、「9」が割当てられている。descriptor_lengthは、このdescriptor_lengthの直後に続くディスクリプタのデータバイト数を規定するためのデータである。CA_system_IDは、関連するECM又はEMMデータを生成及び適用した限定受信システム(CAシステム)の種類を示すデータである。CA_PIDは、CA_system_IDによって規定される限定受信システム(CAシステム)についてのECM又はEMMデータを含んでいるトランスポートストリームのPIDを示す。

条件付きアクセスディスクリプタCA_descriptor()のCA_PIDによって指定されるパケットに記述されているデータ内容は、このCA_descriptor()のコンテキスト(文脈)によって異なってくる。図20を参照して、このCA_PIDが指定するパケットについて説明する。

まず、CA_PIDによって指定されるパケットに記述されているデータ内容は、このCA_descriptor()が、条件付きアクセステーブルCATで使用されているかプログラムマップテーブルにおいて使用されているかによって異なってくる。具体的には、CA_descriptor()が条件付きアクセステーブルに存在する場合には、CA_PIDは、EMMデータが含まれるト

ransport Streamのパケットを示す。CA_descriptor()がプログラムマップテーブルに存在する場合には、CA_PIDは、ECMデータが含まれるTransport Streamのパケットを示す。

さらに、CA_PIDによって指定されるパケットに記述されているデータ内容は、条件付きアクセスディスクリプタCA_descriptor()のプログラムマップテーブル内のコンテキストに応じても、データ内容が異なってくる。この条件付きアクセスディスクリプタCA_descriptor()のプログラムマップテーブル内のコンテキストとは、このCA_descriptor()が、最初のfor文内(図15)において使用されているディスクリプタで使用されているか第2番めのfor文内(図15)において使用されているかということである。

この条件付きアクセスディスクリプタCA_descriptor()が、最初のfor文内で使用されている場合には、CA_PIDは、ECMデータが含まれるTransport StreamパケットのPIDを示す。つまり、この場合、この第1のCA_descriptor()は、program_numberで規定されたプログラムが含まれるTransport StreamパケットとECMデータが含まれるTransport Streamパケットとの対応を記述するためのシンタックスである。つまり、program_numberで規定されたプログラムに含まれる全てのデータエレメントに対して、同じECMデータが割り当てられているということである。言い換えると、プログラムに含まれる全てのデータエレメントに対して同じスクランブルキーを使用してスクランブル処理及びデスクランブル処理が行われていることを示す。

一方、この条件付きアクセスディスクリプタCA_descriptor()が、第2番めのfor文内で使用されている第2のCA_descriptor()である場合には、同じように、CA_PIDは、ECMデータが含まれるTransport StreamパケットのPIDを示す。しかしながら、この第2のCA_descriptor()は、program_numberで規定された

プログラム含まれるトランSPORTストリームパケットとECMデータが含まれるトランSPORTストリームパケットとの対応を記述しているのではなく、このCA_descriptor()は、elementary_PIDで規定されたデータエレメントが含まれるトランSPORTストリームパケットと、ECMデータが含まれるトランSPORTストリームパケットとの対応を記述している。つまり、elementary_PIDで規定されたデータエレメント毎に、ECMデータが割り当てられているということである。言い換えると、プログラムに含まれるデータエレメント毎に異なるスクランブルキーを使用してスクランブル処理及びデスクランブル処理が行われていることを示す。このように、データエレメント毎に異なるスクランブルキーを使用するということは、例えば、1チャンネルのビデオデータと主音声と副音声からなる2チャンネルのオーディオデータから成るプログラムを想定した場合に、副音声のみに異なるスクランブルキーを使用してスクランブルをかけることができる。

次にEMMデータ及びECMデータについて説明する。

EMM(Entitlement Management Message)データは、視聴者が契約した番組等を示す契約情報やスクランブルキーKsを暗号化するために使用したワークキーKwを含んだデータである。EMMデータは、プログラムアソシエーションテーブルPATやプログラムマップテーブルPMTや条件付きアソシエーションテーブルCATと同じように、トランSPORTストリームパケットのペイロードに挿入されて伝送される。以下の説明において、このEMMデータを含むトランSPORTストリームパケットを、EMMパケットと呼ぶことにする。

EMMパケットは、図21のように、4バイトのヘッダと、183バイトのペイロード部とから構成されている。EMMパケットのヘッダは、すでに説明したトランSPORTストリームのパケットと同じように、sync_byte、transport_error_indicator、payload_unit_start_indicator、transport_pri-

riority、PID、transport_scrambling_control、adaptation_field_control、及びcontinuity_counter等のデータフィールドから構成されている。183バイトのペーロード部は、EMMセクションヘッダ部と、EMMデータ部と、CRC部と、スタッフィングバイト部とから構成されている。

EMMセクションヘッダは、table_id、section_syntax-tax_indicator、reserved_0、reserved_1、section_length、table_id_extension、reserved_2、version_number、current_next_indicator、section_number、及びlast_section_number等のデータフィールドから構成されている。

table_idは、各テーブル（各セクション）に対して割当てられた固有の識別番号である。このEMMセクションの識別番号としては、「0x40」から「0xFE」までのユーザ定義可能なtable_idが割当てられている。

section_syntax-tax_indicatorは、「1」に固定された定数である。section_lengthは、このsection_lengthの後のビットからCRCセクションの最後のバイトまでのバイト数を示すデータフィールドである。table_id_extensionは、このEMMセクションの拡張データがあるか無いかを示すデータである。version_numberは、EMMセクションのバージョン番号を示すデータである。トランスポートストリームにおいてこのEMMセクションのパラメータが変化する場合にこのバーション番号がインクリメントされる。current_next_indicatorは、伝送されているEMMセクションが現在使用可能であるか否かを示すデータである。section_numberは、このEMMセクションの番号を示すデータであって、常に、「1」である。EMM1last_section_numberは、このEMMセクションの中で最後のセクションのセクション番号を示すデータであって、常に「1」である。

EMMデータ部は、card_ID、EMM_type、CA_system_ID、Kw_No、Kw、authorize_type、service_ID、series_ID、event_ID、及びcomponent_map等のデータフィールドから構成されている。

card_IDは、IRDにセットされた固有のICカードに付与された識別番号であって、この顧客を管理するための識別番号としても使用されている。EMM_typeは、EMMデータの種類を示すデータである。CA_system_IDは、顧客管理システムを含むCAシステムに付与された識別番号である。Kwは、スクランブルキーKsを暗号化するために使用したワークキーを示し、Kw_Noは、予め登録された256個のワークキーKwのうち、スクランブルキーKsを暗号化する際に使用されたワークキーがどのワークキーであるかを示す番号である。authorize_type、service_ID、series_ID及びevent_IDは、視聴者がどの番組を契約しているかを示す契約条件である。component_mapは、契約しているプログラムを構成するエレメントにおいて、どのエレメントの契約がなされているかをエレメント毎に示すデータである。

ECM(Entitlement_Control_Message)データは、視聴者が契約したプログラムに施されたスクランブルを解除するためのスクランブルキーKsを含んだデータである。ECMデータは、プログラムアソシエーションテーブルPATやプログラムマップテーブルPMTや条件付きアソシエーションテーブルCATと同じように、トランSPORTストリームパケットのペイロードに挿入されて伝送される。以下の説明において、このECMデータを含むトランSPORTストリームパケットを、ECMパケットと呼ぶことにする。ECMパケットは、約100 msecの周期で伝送され、EMMデータとして伝送されるスクランブルキーは、約4秒毎に新しく更新されるようになっている。

ECMパケットは、図22のように、4バイトのヘッダと、183バイトのペイロード部とから構成されている。ECMパケットのヘッダは、すでに説明した

トランSPORTストリームのパケットと同じように、sync_byte、transport_error_indicator、payload_unit_start_indicator、transport_priority、PID、transport_scrambling_control、adaptation_field_control、及びcontinuity_counter等のデータフィールドから構成されている。183バイトのペーロード部は、ECMセクションヘッダ部と、ECMデータ部と、CRC部と、スタッフィングバイト部とから構成されている。

ECMセクションヘッダは、table_id、section_syntax_indicator、reserved_0、reserved_1、section_length、table_id_extension、reserved_2、version_number、current_next_indicator、section_number、及びlast_section_number等のデータフィールドから構成されている。table_idは、各テーブル（各セクション）に対して割当てられた固有の識別番号である。このECMセクションの識別番号としては、「0x40」から「0xF0」までのユーザ定義可能なtable_idが割当てられている。section_syntax_indicatorは、「1」に固定された定数である。section_lengthは、このsection_lengthの後のビットからCRCセクションの最後のバイトまでのバイト数を示すデータフィールドである。table_id_extensionは、このECMセクションの拡張データがあるか無いかを示すデータである。version_numberは、ECMセクションのバージョン番号を示すデータである。トランSPORTストリームにおいてこのECMセクションのパラメータが変化する場合にこのバーション番号がインクリメントされる。current_next_indicatorは、伝送されているECMセクションが現在使用可能であるか否かを示すデータである。section_numberは、この

ECMセクションの番号を示すデータであって、常に、「1」である。ECM last_section_numberは、このECMセクションの中で最後のセクションのセクション番号を示すデータであって、常に「1」である。

ECMデータ部は、ECM_type、CA_system_ID、Kw_No、service_mode、service_ID、series_ID、event_ID、component_map、Ks_Odd及びKs_Even等のデータフィールドから構成されている。

ECM_typeは、ECMデータの種類を示すデータである。CA_system_IDは、顧客管理システムを含むCAシステムに付与された識別番号である。Kw_Noは、予め登録された256個のワークキーKwのうち、スクランブルキーKsを暗号化する際に使用されたワークキーがどのワークキーであるかを示す番号である。service_mode、service_ID、series_ID及びevent_IDは、視聴者がどの番組を契約しているかを示す契約条件である。component_mapは、契約しているプログラムを構成するエレメントにおいて、どのエレメントの契約がなされているかをエレメント毎に示すデータである。Ks_Odd及びKs_Evenは、伝送されたビデオデータ及びオーディオデータをスクランブルするために使用したスクランブルキーである。スクランブルキーは、奇数キーKs_Oddと偶数キーKs_Evenから構成され、奇数キーと偶数キーとが4秒毎に交互にスクランブルとして使用される。

次に、図23を参照して、受信機として設けられたIRD (Integrated_Receiver_Decoder) 20について詳細に説明する。

このIRDは、衛星を介して伝送された変調ストリームを復調するための復調回路21と、復調回路21において復調されたストリームをパケットの種類に応じて分離するデマルチプレクサ22と、デマルチプレクサ22によって分離されたPATパケット、PMTパケット、CATパケット、EMMパケット、及びE

CMパケットを受け取るCPU23と、暗号化ワークキーKw' と暗号化スクランブルキーKs' の暗号を解読するためのセキュリティモジュール24と、スクランブルされたビデオストリーム、オーディオストリーム及びプライベートデータストリームのスクランブルを解除するデスクランプラー25V、25A及び25Pと、ビデオストリーム及びオーディオストリームを復号化するデコーダ26V、26Aとを有している。

デマルチプレクサ22は、CPU23から制御コマンドを受取り、このコマンドに応答して適切なトランSPORTストリームパケットを適切なタイミングでCPU23に供給する機能を有している。

CPU23は、デマルチプレクサ22から供給されたPATパケットを解析するPATパケット解析部231と、デマルチプレクサ22から供給されたPMTパケットを解析するPMTパケット解析部232と、デマルチプレクサ22から供給されたCATパケットを解析するCATパケット解析部233、デマルチプレクサ22から供給されたEMM' パケットを解析するEMMパケット解析部234と、デマルチプレクサ22から供給されたECM' パケットを解析するECMパケット解析部235とを有している。

PAT解析部231は、デマルチプレクサ22からPATパケットとして供給されたトランSPORTストリームパケットを解析することによって、このPATパケットに含まれているprogram_numberとprogram_map_PIDを得る。また、PAT解析部231は、セキュリティモジュール24から受信者が契約しているプログラムがどのプログラムであるかを示すauthorize_typeを受け取る。そして、PAT解析部231は、セキュリティモジュールから供給されたauthorize_typeとデマルチプレクサ22から供給されたprogram_numberとを比較し、視聴者が契約しているプログラムと一致したprogram_numberに対応したprogram_map_PIDのみを選択する。その結果、PAT解析部231は、視聴者が契約しているプログラムに対応したプログラムマップテーブルの

P I Dのみを得ることができる。

続いて、デマルチプレクサ22は、PAT解析部231から供給された program_map_PIDによって指定されたP I Dを有したトランSPORTストリームパケットを選択し、その選択されたトランSPORTストリームパケットをPMTパケットとしてPMT解析部232に出力する。

PMT解析部232は、program_map_PIDによって指定されたP I Dを有したMPMTパケットに含まれるPMTデータを解析する。具体的には、PMT解析部232は、PMTパケットのPMTデータとして記述された elementary_PIDから、program_numberによって指定されたプログラムを構成するデータエレメントが含まれたトランSPORTストリームパケットのP I Dを得る。例えば、プログラムがビデオデータとオーディオデータの2つのデータエレメントから構成されるとすると、第1のelementary_PIDによってビデオストリームが含まれるトランSPORTストリームパケットを指定し、第2のelementary_PIDによってオーディオストリームが含まれるトランSPORTストリームパケットを指定するということである。

さらに、このPMT解析部232は、PMTデータ中にdescriptor()関数として記述されたCA_descriptorを参照する。そして、このPMT解析部232は、このCA_descriptor中に記述されたCA_P I Dを得て、このCA_P I Dをデマルチプレクサ22にフィードバックする。このCA_descriptor中に記述されたCA_P I Dは、ECMデータが含まれたトランSPORTストリームパケットのP I Dを示すデータである。

続いて、デマルチプレクサ22は、PMT解析部232から供給された、elementary_PIDによって指定されたP I Dを有したトランSPORTストリームパケットを適切な処理回路に出力する。例えば、データエレメントがビデオストリームであれば、ビデオストリームをデスクランプするためのデス

クランブル回路 2 5 V に出力し、データエレメントがオーディオストリームであれば、オーディオストリームをデスクランブルするためのデスクランブル回路 2 5 A に出力し、データエレメントがプライベートデータストリームであれば、プライベートデータストリームをデスクランブルするためのデスクランブル回路 2 5 P に出力する。

さらに、デマルチプレクサ 2 2 は、C A _ P I D によって指定された P I D を有したトранSPORTストリームパケットを、E C M パケットとして E C M 解析部 2 3 5 に供給する。よって、E C M 解析部 2 3 5 に供給される E C M データは、視聴者が契約しているプログラムに関する E C M データのみである。

E C M 解析部 2 3 5 は、まず、デマルチプレクサ 2 2 から受け取った E C M パケットをフィルタリングする。具体的には、E C M 解析部 2 3 5 は、この E C M データ部内の C A _ s y s t e m _ I D とセキュリティモジュール 2 4 から供給された C A _ s y s t e m _ I D とを比較し、セキュリティモジュール 2 4 から供給された C A _ s y s t e m _ I D と一致する C A _ s y s t e m _ I D とを含んだ E C M パケットのみを選択する。次に、E C M 解析部 2 3 5 は、この選択された E C M パケットに含まれる E C M データを解析することによって、暗号化スクランブルキー k s ' を得ることができる。E C M 解析部 2 3 5 は、この暗号化スクランブルキー K s ' を、セキュリティモジュール 2 4 内のマイクロプロセッサ M P U 内の暗号解読回路 2 4 2 に供給する。

一方、デマルチプレクサ 2 2 は、伝送されたビットストリーム中から、C A T パケットの P I D を有したトランSPORTストリームパケットを検出し、その検出したトランSPORTストリームパケットを C A T パケットとして C A T 解析部 2 3 3 に出力する。

C A T 解析部 2 3 3 は、まず、デマルチプレクサ 2 2 から受け取った C A T パケットに含まれる C A _ d e s c r i p t o r () 関数を検出し、C A _ d e - s c r i p t o r () 関数内の C A _ P I D から、C A T パケットの C A _ d e s c r i p t o r () によって指定されたトランSPORTストリームパケッ

トのP I Dを得る。このC A TパケットのC A _ d e s c r i p t o r () によって指定されたトランSPORTストリームパケットが、EMM情報を含んだトランSPORTストリームパケットである。

デマルチプレクサ22は、ビットストリーム中から、C A T解析部233から受け取ったC A _ P I Dによって指定されたP I Dを有したトランSPORTストリームパケットを選択して、その選択されたトランSPORTストリームパケットをEMM'パケットとしてEMM解析部234に供給する。

EMM解析部234は、まず、デマルチプレクサ212から受け取ったEMM'パケットをフィルタリングして、このセキュリティモジュールに対応したEMM'パケットのみを選択する。具体的には、デマルチプレクサ22から受け取ったEMMパケットのC A _ d e s c r i p t o r () のC A _ P I Dによって指定されたトランSPORTストリームパケットは、EMMデータを含んだ全てのEMM'パケットであるので、このC A _ P I Dを参照することによって、EMM'パケットに含まれるEMMデータを得ることができる。EMM解析部234は、このEMMデータ部内のC a r d _ I DとC A _ s y s t e m _ I Dと、セキュリティモジュール24のメモリ241から供給されたC a r d _ I DとC A _ s y s t e m _ I Dとを比較し、セキュリティモジュール24から供給されたC a r d _ I DとC A _ s y s t e m _ I Dとそれぞれ一致するC a r d _ I DとC A _ s y s t e m _ I Dとを含んだEMM'パケットのみを選択する。

次に、EMM解析部234は、この選択したEMMパケットに含まれる101バイトのEMMデータを、最新のEMMデータとしてセキュリティモジュール24のメモリ241に供給し、メモリ241内の古いEMMデータを更新する。さらに、EMM解析部234は、このEMMデータに含まれる暗号化ワークキーK_{w'}を、セキュリティモジュール24内のマイクロプロセッサM P U内の暗号解読回路242に供給する。

セキュリティモジュール24は、メモリ241と第1の暗号解読回路242及び第2の暗号解読回路243を備えたマイクロプロセッサとから構成されている

。このセキュリティモジュール24は、例えば、IRD本体に対して着脱可能なICカードで構成されている。

セキュリティモジュール24の第1の暗号解読回路242は、EMM解析部234から暗号化ワークキーKw'を受取り、予め記憶されたマスターキーKmによってこの暗号化ワークキーKw'の暗号を解読する。そして、第1の暗号解読回路242は、この暗号解読されたワークキーKwを、暗号化第2の暗号解読回路243に供給する。

セキュリティモジュール24の第2の暗号解読回路242は、ECM回路235から暗号化スクランブルキーKs'を受取ると共に、第1の暗号解読回路242から暗号解読されたワークキーKwを受取り、この暗号解読されたワークキーKwによって、暗号化スクランブルキーKs'の暗号を解読する。暗号解読されたスクランブルキーKsは、デスクランブル25V、25A及び25Pに供給される。ここでは、デスクランブル25V、25A及び25Pに同じスクランブルキーKsを供給する場合について説明したが、もし、各データエレメント毎に異なるスクランブルキーKsが設定されている場合には、各デスクランブルに対してそれぞれ異なるスクランブルキーKsが供給される。

以上の構成において、トランSPORTストリームパケット構成の複数のデータエレメントからなるプログラムデータの上記各トランSPORTストリームパケットを多重化して送信するデータ多重化装置において、1つのプログラムを構成する複数のデータエレメントのうち、1つ又は複数のデータエレメントに対応したスクランブルキーを生成し、各データエレメントごとにスクランブルをかけることにより、視聴者はデータエレメントごとに視聴契約を結ぶことができる。

また、多重化された各トランSPORTストリームパケットに対してそれぞれ対応するスクランブルキーを用いてスクランブルをかけることにより、各トランSPORTストリームパケットを多重化する前にスクランブルをかける場合に比べて、スクランブルをかけるための回路構成が簡単になる。

また、各バッファメモリに入力されるデータエレメントの入力レートが基準レ

ートに比べて高いとき、複数のバッファメモリのうち、優先順位の低い情報をバッファリングするバッファメモリを切り換え対象から除外してスイッチ手段を切り換え制御することにより、優先順位の高いデータエレメントをバッファリングするバッファメモリがオーバーフローすることを未然に防止し得る。

また、受信装置側では、スクランブルキーを用いて当該スクランブルキーに対応するデータエレメントごとにそのトランSPORTストリームパケットをデスクランブルすることにより、データエレメントごとに個別にスクランブルを解除することができる。

かくして以上の構成によれば、視聴者は必要とするデータエレメントのみを契約して視聴することができるデータ多重化装置を簡単な構成によつて実現できる。

また優先順位の低いデータエレメントを選択対象から除外して必要なデータエレメントを優先的に選択して多重化することにより、バッファメモリのオーバーフローを有効に回避することができる。

産業上の利用可能性

本発明は、MPEG2を用いてビデオデータやオーディオデータを圧縮符号化し、その符号化されたストリームを地上波や衛星波を介して放送するデジタル放送システムに利用できる。

請求の範囲

1. トランSPORTストリームパケット構成の複数のデータエレメントからなるプログラムデータの上記各トランSPORTストリームパケットを多重化して送信するデータ多重化装置において、

上記データエレメントごとに対応するスクランブルキーを生成するスクランブルキー生成手段と、

上記スクランブルキー生成手段によって生成されたスクランブルキーを用いて対応する上記データエレメントのトランSPORTストリームパケットにスクランブルをかけるスクランブル手段と

を備えることを特徴とするデータ多重化装置。

2. 上記スクランブルキー生成手段は、

上記1つのプログラムを構成する上記複数のデータエレメントのうち、1つ又は複数のデータエレメントに対応したスクランブルキーを生成することを特徴とする請求の範囲第1項に記載のデータ多重化装置。

3. 上記プログラムを構成する複数のデータエレメントは、ビデオデータ、メインオーディオデータ、サブオーディオデータ及びプライベートデータであることを特徴とする請求の範囲第1項に記載のデータ多重化装置。

4. 上記スクランブル手段は、

上記多重化された各トランSPORTストリームパケットに対してそれぞれ対応する上記スクランブルキーを用いてスクランブルをかけることを特徴とする請求の範囲第1項に記載のデータ多重化装置。

5. 上記スクランブル手段は、

上記各トランSPORTストリームパケットを表すパケット識別コードとその対応するスクランブルキーとの対応表を用いて上記各トランSPORTストリームパケットにスクランブルをかけるための各スクランブルキーを検索することを特徴とする請求の範囲第4項に記載のデータ多重化装置。

6. 上記データ多重化装置は、

ワークキーを用いて上記スクランブルキーを暗号化する第1の暗号化手段を具え、上記暗号化されたスクランブルキーを上記各トランSPORTストリームパケットと共に多重化して送信する

ことを特徴とする請求の範囲第4項に記載のデータ多重化装置。

7. 上記データ多重化装置は、

マスターキーを用いて上記ワークキーを暗号化する第2の暗号化手段を具え、上記暗号化されたワークキーを上記各トランSPORTストリームパケットと共に多重化して送信する

ことを特徴とする請求の範囲第6項に記載のデータ多重化装置。

8. 複数のデータエレメントを構成する複数のパケットデータを格納する複数のバッファメモリと、

上記バッファメモリを切り換えるスイッチ手段を有し、当該スイッチ手段によって上記バッファメモリを順次時分割に切り換えることによって上記複数のパケットデータ列を時分割に多重化して出力する多重化手段と、

上記スイッチ手段による切り換え対象である上記複数のバッファメモリを、上記パケットデータ列の入力レートに応じて選択するスイッチ制御手段とを備えることを特徴とするデータ多重化装置。

9. 上記スイッチ制御手段は、

上記入力レートが基準レートに比べて高いとき、上記複数のバッファメモリのうち、優先順位の低い情報をバッファリングするバッファメモリを切り換え対象から除外して上記スイッチ手段を切り換え制御する

ことを特徴とする請求の範囲第8項に記載のデータ多重化装置。

10. 上記スイッチ制御手段は、

EMMデータを含むパケットデータを上記優先順位の低い情報として上記EMMデータを含むパケットデータをバッファリングするバッファメモリを上記切り換え対象から除外する

ことを特徴とする請求の範囲第9項に記載のデータ多重化装置。

11. 上記スイッチ制御手段は、

上記EMMデータを含むパケットデータをバッファリングするバッファメモリを上記切り換え対象から除外した後、上記入力レートが上記基準レートに比べて依然として高いとき、上記EMMデータを含むパケットデータをバッファリングするバッファメモリに加えて、EPGデータを含むパケットデータをバッファリングするバッファメモリを上記切り換え対象から除外する

ことを特徴とする請求の範囲第10項に記載のデータ多重化装置。

12. 複数のデータエレメントから構成されるプログラムを配信するプログラム配信システムにおいて、顧客のプログラム毎及びデータエレメント毎の契約を管理するための顧客管理システムと、上記プログラムに含まれるデータエレメントをデスクランブルする際に使用するスクランブルキーを上記データエレメント毎に生成する視聴許可システムと、

上記複数のプログラムに含まれるデータエレメントをそれぞれ符号化し、その符号化データエレメントから構成される符号化ストリームを上記各プログラム毎に生成する符号化システムと、上記符号化手段から各プログラム毎に出力された

符号化ストリームを多重化する多重化手段と、上記視聴許可システムにおいて生成されたスクランブルキーに基いて、上記多重化ストリームに含まれる符号化データエレメントに対して各データエレメント毎に選択的にスクランブルをかけるスクランブル手段とを備えたマルチプレクサシステムと、
を備えたことを特徴とするプログラム配信システム。

1 3. 上記顧客管理システムは、

上記スクランブルキーを暗号化するためのワークキーを生成し、
上記顧客を識別するための顧客識別番号及び上記ワークキーを、ＥＭＭデータとして上記視聴許可システムに供給することを特徴とする請求の範囲第1 2項に記載のプログラム配信システム。

1 4. 上記視聴許可システムは、

上記ＥＭＭデータとして供給されたワークキーを、マスターキーを使用して暗号化し、暗号化ワークキーを出力する第1の暗号化手段を有していることを特徴とする請求の範囲第1 3項に記載のプログラム配信システム。

1 5. 上記視聴許可システムは、

上記第1の暗号化手段によって暗号化された暗号化ワークキー及び上記顧客識別番号を、暗号化ＥＭＭデータとして上記マルチプレクサシステムに供給することを特徴とする請求の範囲第1 4項に記載のプログラム配信システム。

1 6. 上記視聴許可システムは、

上記第1の暗号化手段において暗号化された暗号化ワークキーを識別するためのワークキー識別番号と、上記スクランブルキーとをＥＣＭデータとして上記マルチプレクサシステムに供給することを特徴とする請求の範囲第1 5項に記載のプログラム配信システム。

1 7. 上記視聴許可システムは、

上記ワークキーと、該ワークキーを識別するためのワークキー識別番号とをそれぞれ対応付けて登録したワークキーテーブルを備え、

該ワークキーテーブルを上記マルチプレクサシステムに供給することを特徴とする請求の範囲第16項に記載のプログラム配信システム。

1 8. 上記マルチプレクサシステムは、

上記ECMデータに含まれるスクランブルキーを上記ワークキーを使用して暗号化し、暗号化スクランブルキーを出力するための第2の暗号化手段を有していることを特徴とする請求の範囲第17項に記載のプログラム配信システム。

1 9. 上記第2の暗号化手段は、

上記スクランブルキーを暗号化するする際に使用されるワークキーは、上記暗号化EMMデータに含まれている暗号化ワークキーでは無く、上記視聴許可システムから供給されたワークキーテーブルから得られる暗号化されていないワークキーであることを特徴とする請求の範囲第18項に記載のプログラム配信システム。

2 0. 上記第2の暗号化手段は、

上記視聴許可システムから供給されたワークキーテーブルを参照することによって、上記ECMデータに含まれるワークキー識別番号からワークキーを得、

上記第2の暗号化手段において、上記ワークキーテーブルから得られたワークキーを使用して上記ECMデータに含まれるスクランブルキーを暗号化し、

上記第2の暗号化回路において暗号化された暗号化スクランブルキーを、暗号化ECMデータとして出力することを特徴とすることを特徴とする請求の範囲第19項に記載のプログラム配信システム。

2 1. 上記符号化システムから出力される符号化ストリーム、上記視聴許可システムから出力される暗号化 E MM データ及び E CM データは、トランSPORTストリームパケットの形態で出力され、上記トランSPORTストリームパケットのには、トランSPORTストリームパケットを識別するためのパケット I D が付与されていることを特徴とする請求の範囲第 2 0 項に記載のプログラム配信システム。

2 2. 上記マルチプレクサシステムは、

上記 E CM データに含まれるスクランブルキーを暗号化し、上記多重化手段に暗号化 E CM データとして出力するための第 2 の暗号化手段をさらに備えたことを特徴とする請求の範囲第 2 1 項に記載のプログラム配信システム。

2 3. 上記スクランブル手段は、

上記暗号化 E MM データ及び上記暗号化 E CM データはスクランブルせずに、上記プログラムを構成する複数のデータエレメントのみをスクランブルすることを特徴とする請求の範囲第 2 2 項に記載のプログラム配信システム。

2 4. 上記スクランブル手段は、

上記データエレメントを含んだトランSPORTストリームパケットのパケット I D と上記データエレメントに対してそれぞれ設定されたスクランブルキーとを対応付けたテーブルに基いて、上記データエレメントに対応付けられたスクランブルキーを使用して、上記データエレメントをスクランブルすることを特徴とする請求の範囲第 2 2 項に記載のプログラム配信システム。

2 5. 上記スクランブル手段は、

上記多重化手段から上記スクランブル手段に供給されたトランSPORTストリームパケットの全てのトランSPORTストリームパケットのパケット I D を検出

し、

上記パケットIDと上記スクランブルキーとを対応付けたテーブルに基いて、上記検出されたパケットIDに対してスクランブルキーが設定されているか否かを判断し、

上記パケットIDに対してスクランブルキーが設定されている場合には、上記パケットIDによって示されるトранSPORTストリームパケットに含まれるデータエレメントを、設定されたスクランブルキーを使用してスクランブルし、

上記パケットIDに対してスクランブルキーが設定されていない場合には、上記パケットIDによって示されるトランSPORTストリームパケットに含まれるデータはスクランブルしないことを特徴とする請求の範囲第22項に記載のプログラム配信システム。

26. 上記マルチプレクサシステムは、

上記ECMデータに含まれるスクランブルキーを暗号化するための第2の暗号化手段と、上記マルチプレクサシステムにトランSPORTストリームパケットの形態で供給されたデータをそれぞれバッファリングし、トランSPORTストリームパケットの単位の上記多重化手段に出力するバッファ手段をさらに備えたことを特徴とする請求の範囲第20項に記載のプログラム配信システム。

27. 上記マルチプレクサシステムは、

上記データエレメントを含んだトランSPORTストリームパケットをバッファリングするための複数のバッファのバッファ残量を監視し、

上記データエレメントを含んだトランSPORTストリームパケットをバッファリングするための複数のバッファのいずれかがオーバーフローしそうなときには、上記EMMデータを含んだトランSPORTストリームパケットをバッファリングするためのバッファからEMMデータを含んだトランSPORTストリームパケットを上記多重化手段に出力する代わりに、上記オーバーフローしそうなバッファ

から上記データエレメントを含んだトランSPORTストリームパケットを上記多重化手段に出力することを特徴とする請求の範囲第26項に記載のプログラム配信システム。

28. 上記マルチプレクサシステムから出力されたトランSPORTストリームを、伝送路を介して受信側に配信する配信システムと、

上記伝送路を介して伝送されたトランSPORTストリームを受信する受信システムとをさらに備えていることを特徴とする請求の範囲第20項に記載のプログラム配信システム。

29. 上記受信システムは、

上記伝送されたトランSPORTストリームをデマルチプレクスするデマルチプレクサと、上記スクランブルされた各データエレメントを、供給されたスクランブルキーを使用してそれぞれデスクランブルするデスクランブラーと、

上記デスクランブルされたデータをデータエレメント毎にそれぞれデコードするデコーダと、上記トランSPORTストリームを構成するトランSPORTストリームパケットを解析するC P Uと、上記トランSPORTストリームに含まれる暗号化スクランブルキーを解読し、暗号解読されたスクランブルキーを上記デスクランブラーに供給するセキュリティモジュールと、

を備えたことを特徴とする請求の範囲第28項に記載のプログラム配信システム。

30. 上記セキュリティモジュールは、

上記伝送されたトランSPORTストリームに含まれる暗号化E M Mデータに含まれる自己の契約情報を記憶するメモリ手段と、

上記伝送されたトランSPORTストリーム中に含まれる暗号化ワークキーと上記顧客管理システムにおいて使用されたマスターキーと同じマスターキーを受取

り、上記マスターキーを使用して上記暗号化ワークキーの暗号を解読する第1の暗号解読手段と、

上記トランSPORTストリーム中に含まれる暗号化スクランブルキーと上記第1の暗号解読手段から供給された暗号解読されやワークキーとを受取り、上記暗号解読されたワークキーを使用して上記暗号化スクランブルの暗号を解読する第2の暗号解読手段と、

を備えたことを特徴とする請求の範囲第29項に記載のプログラム配信システム。

3 1. 上記CPUは、

上記デマルチプレクサから供給された暗号化ECMデータを含んだトランSPORTストリームパケットから、受信者が契約しているプログラム又はデータエレメントに関する暗号化ECMデータを有するトランSPORTストリームパケットのみをフィルタリングし、

上記フィルタリングされたトランSPORTストリームパケットに含まれる暗号化ECMデータを解析することによって、上記暗号化ECMデータから上記暗号化スクランブルキーを得ることを特徴とする請求の範囲第30項に記載のプログラム配信システム。

3 2. 上記セキュリティモジュールは、

上記CPUから上記プログラムに対応付けられた暗号化スクランブルキーが供給された場合には、供給された暗号化スクランブルキーの暗号を解読し、上記プログラムを構成する複数のデータエレメントに対応する複数のデスクランブルーに対して同じスクランブルキーをそれぞれ供給し、

上記CPUから上記複数のデータエレメントにそれぞれ対応付けられた複数の暗号化スクランブルキーが供給された場合には、供給された複数の暗号化スクランブルキーの暗号をそれぞれ解読し、上記複数のデータエレメントのうち契約し

ているデータエレメントに対応する複数のデスクランプラーに対して、それぞれ異なるスクランブルキーを供給することを特徴とする請求の範囲 3 1 項に記載のプログラム配信システム。

3 3 . 上記視聴許可システムは、

上記スクランブルキーを暗号化するために使用されるワークキーをマスターキーを使用して暗号化するための第 1 の暗号化手段を備え、

上記第 1 の暗号化手段によって暗号化された暗号化ワークキーと上記顧客を識別するための顧客識別番号とを、暗号化 EMM データとして上記マルチプレクサシステムに供給し、

上記暗号化手段において暗号化されたワークキーを識別するためのワークキー識別番号と上記スクランブルキーとを、 ECM データとして上記マルチプレクサシステムに供給する

ことを特徴とする請求の範囲第 1 2 項に記載のプログラム配信システム。

3 4 . 上記複数のプログラム、上記プログラムを構成する複数のデータエレメント、上記複数の ECM データ及び上記複数の EMM データをどのように多重化するかを示すプログラム仕様情報を生成し、この生成されたプログラム使用情報にに対応するように、上記複数のプログラム、上記複数のデータエレメント、上記複数の ECM データ及び上記複数の EMM データを多重化するように上記エンコーダシステム及び上記マルチプレクサシステムを制御する、エンコーダ／マルチプレクサコントロールシステムを備えたことを特徴とする請求の範囲第 3 3 項に記載のプログラム配信システム。

3 5 . 上記データ配信システムから出力されるトランSPORTストリーム内において、上記記プログラムを構成する複数のデータエレメントが含まれるトランSPORTストリームパケット、上記 ECM データが含まれるトランSPORTストリ

ームパケット及び上記E MMデータが含まれるトランSPORTストリームパケットのパケットIDを識別するためのプログラム仕様情報を生成し、

このプログラム使用情報に対応するように、上記記プログラムを構成する複数のデータエレメントが含まれるトランSPORTストリームパケット、上記E CMデータが含まれるトランSPORTストリームパケット及び上記E MMデータが含まれるトランSPORTストリームパケットを多重化するように、上記エンコーダシステム及び上記マルチプレクサシステムを制御するエンコーダ／マルチプレクサコントロールシステムを備えたことを特徴とする請求の範囲第33項に記載のプログラム配信システム。

3 6. 上記エンコーダシステムは、上記各符号化されたデータエレメンをそれぞれトランSPORTストリームパケットの形態を有したエレメンタリパケットとして上記マルチプレクサシステムに供給し、上記視聴許可システムは、上記暗号化E MMデータ及び上記E CMデータを、それぞれ、トランSPORTストリームパケットの形態を有した暗号化E MMパケット及びE CMパケットとして上記マルチプレクサシステムに供給し、

上記エンコーダ／マルチプレクサコントロールシステムは、上記プログラム仕様情報を、トランSPORTストリームパケットの形態を有したPSIパケットとして上記マルチプレクサシステムに供給することを特徴とする請求の範囲第34項に記載のプログラム配信システム。

3 7. 上記マルチプレクサシステムは、

上記多重化手段の前段に、上記E CMデータに含まれるスクランブルキーを暗号化するための第2の暗号化手段をさらに備えたことを特徴とする請求の範囲第36項に記載のプログラム配信システム。

3 8. 上記視聴許可システムは、

上記ワークキーと、該ワークキーを識別するためのワークキー識別番号とをそれぞれ対応付けたワークキーテーブルを上記マルチプレクサシステムの上記第2の暗号化手段に供給することを特徴とする請求の範囲第37項に記載のプログラム配信システム。

3 9. 上記第2の暗号化手段は、

上記ECMデータに含まれるワークキー識別番号から、上記ワークキーテーブルを参照することによってワークキーを得、

上記第2の暗号化手段において、上記ワークキーテーブルから得られたワークキーを使用して上記ECMデータに含まれるスクランブルキーを暗号化し、上記第2の暗号化回路において暗号化された暗号化スクランブルキーを、暗号化ECMデータとして上記多重化手段に供給することを特徴とする請求の範囲第38項に記載のプログラム配信システム。

4 0. 上記エンコーダ／マルチプレクサコントロールシステムは、

上記マルチプレクサシステムにトランSPORTストリームパケットの形態として供給される全てのトランSPORTストリームパケットに対して、上記トランSPORTストリームパケットを識別するためのパケットIDを付与することを特徴とする請求の範囲第39項に記載のプログラム配信システム。

4 1. 上記プログラム仕様情報は、

少なくとも、プログラムアソシエーションテーブルと、プログラムマップテーブルと、コンディショナルアクセステーブルとから構成されていることを特徴とする請求の範囲第40項に記載のプログラム配信システム。

4 2. 上記エンコーダ／マルチプレクサコントロールシステムは、

上記プログラムアソシエーションテーブルを含んだトランSPORTストリーム

パケットを P A T パケットとして上記マルチプレクサシステムに供給し、
上記プログラムマップテーブルを含んだトランSPORTストリームパケットを
P M T パケットとして上記マルチプレクサシステムに供給し、
上記コンディショナルアクセステーブルを含んだトランSPORTストリームパ
ケットを C A T パケットとして上記マルチプレクサシステムに供給することを特
徴とする請求の範囲第 4 1 項に記載のプログラム配信システム。

4 3. 上記プログラムアソシエーションテーブルは、プログラム番号とそのプロ
グラム番号に対応する P M T パケットのパケット I D を指定するためのテーブル
であって、

上記プログラムマップテーブルは、プログラムを構成する複数のデータエレメ
ントが含まれるトランSPORTストリームパケットのパケット I D をそれぞれ指
定するためのテーブルであって、上記コンディショナルアクセステーブルは、上
記暗号化 E M M パケットのパケット I D を指定するためのテーブルであることを
特徴とする請求の範囲第 4 2 項に記載のプログラム配信システム。

4 4. 上記プログラムアソシエーションテーブルには、
プログラムを示すプログラム番号と該プログラムに関連付けられた P M T パケ
ットのパケット I D とが記述され、

上記プログラムマップテーブルには、
上記プログラムを示すプログラム番号と、上記プログラムを構成する複数のデ
ータエレメントが含まれるトランSPORTストリームパケットが含まれる複数の
パケット I D と、上記プログラム又は上記データエレメントと関連付けられた暗
号化 E C M パケットのパケット I D を指定するためのディスクリプタとが記述さ
れている

ことを特徴とする請求の範囲第 4 3 項に記載のプログラム配信システム。

4 5. 上記プログラムマップテーブル中の上記ディスクリプタが、上記プログラ

ム番号と対応つけられた位置に記述されている場合には、上記ディスクリプタは、上記プログラムを構成する複数のデータエレメントの全てのデータエレメントをスクランブルするためのスクランブルキーを含んだECMパケットのパケットIDを指定し、

上記プログラムマップテーブル中の上記ディスクリプタが、上記プログラムの各データエレメントと対応付けられた位置にそれぞれ記述されている場合には、上記プログラムを構成する複数のデータエレメントの各データエレメントをそれぞれスクランブルするための複数のスクランブルキーを含んだ複数のECMパケットのパケットIDを指定することを特徴とする請求の範囲第44項に記載のプログラム配信システム。

4 6. 上記プログラムが、第1のデータエレメントから第nのデータエレメントを有し、上記第1のデータエレメントから第nのデータエレメントに対して同じスクランブルキーが指定されている場合には、上記プログラムマップテーブルにおいて、

上記プログラムを示すプログラム番号と、上記第1番めのデータエレメントから上記第nのデータエレメントをそれぞれスクランブルするスクランブルキーを含んだECMパケットのパケットIDとが対応付けられて記述されていることを特徴とする請求の範囲第45項に記載のプログラム配信システム。

4 7. 上記プログラムが、第1のデータエレメントから第nのデータエレメントを有し、上記第1のデータエレメントから第nのデータエレメントに対して少なくとも1つの異なるスクランブルキーが指定されている場合には、

上記プログラムマップテーブルにおいて、

第1番めのデータエレメントが含まれるトランSPORTストリームパケットのパケットIDと、上記第1番めのデータエレメントをスクランブルするスクランブルキーを含んだECMデータを含んだトランSPORTストリームパケットのパ

ケット I D とが対応付けられて記述され、

第 n 番めのデータエレメントが含まれるトランSPORTストリームパケットのパケット I D と、上記第 n 番めのデータエレメントをスクランブルするスクランブルキーを含んだ ECM データを含んだトランSPORTストリームパケットのパケット I D とが対応付けられて記述されていることを特徴とする請求の範囲第 4 5 項に記載のプログラム配信システム。

4 8. 上記エンコーダ／マルチプレクサコントロールシステムは、

上記プログラムマップテーブル及び上記コンディショナルアクセステーブルに
対して、固有のパケット I D を指定することを特徴とする請求の範囲第 4 2 項に
記載のプログラム配信システム。

4 9. 上記スクランブル手段は、

上記プログラム仕様情報、上記 EMM データ及び上記 ECM データはスクランブルせずに、上記データエレメントのみをスクランブルすることを特徴とする請求の範囲第 4 2 項に記載のプログラム配信システム。

5 0. 上記スクランブル手段は、

上記データエレメントを含んだトランSPORTストリームパケットのパケット I D と上記データエレメントに対して指定されたスクランブルキーとを対応付けた対応テーブルに基いて、上記データエレメントに対して指定されたスクランブルキーを使用して、上記データエレメントをそれぞれスクランブルすることを特徴とする請求の範囲第 4 2 項に記載のプログラム配信システム。

5 1. エンコーダ／マルチプレクサコントロールシステムは、

上記 ECM パケット、上記 EMM パケット、上記 P S I パケット、上記エレメントタリーパケットをそれぞれ識別するためのパケット I D を指定する際に、各ト

ransport Stream Packetに対して割り当てるPacket IDが重複しない
ように過去の処理において使用したPacket IDを記憶することを特徴とする請
求の範囲第42項に記載のプログラム配信システム。

52. エンコーダ／マルチプレクサコントロールシステムは、

各Transport Stream Packetに対して割り当たされたPacket IDと
、該Transport Stream Packetに含まれるデータをスクランブルする際
に使用するスクランブルキーとを対応付けたテーブルを生成し、

上記Packet IDと上記スクランブルキーとを対応付けたテーブルを、上記マ
ルチプレクサシステムに供給することを特徴とする請求の範囲第42項に記載の
プログラム配信システム。

53. 上記スクランブル手段は、

上記Packet IDと上記スクランブルキーとを対応付けたテーブルを参照する
ことによって、上記プログラム仕様情報、上記EMMデータ及び上記ECMデータ
はスクランブルせずに、上記データエレメントのみをスクランブルすることを
特徴とする請求の範囲第52項に記載のプログラム配信システム。

54. 上記スクランブル手段は、

上記Packet IDと上記スクランブルキーとを対応付けたテーブルを参照する
ことによって、上記データエレメントに対して指定されたスクランブルキーを使
用して、上記データエレメントをそれぞれスクランブルすることを特徴とする請
求の範囲第52項に記載のプログラム配信システム。

55. 上記スクランブル手段は、

上記多重化手段から上記スクランブル手段に供給されたTransport Stream
Packetの全てのTransport Stream PacketのPacket IDを検出

し、

上記パケットIDと上記スクランブルキーとを対応付けたテーブルに基いて、上記検出されたパケットIDに対してスクランブルキーが設定されているか否かを判断し、

上記パケットIDに対してスクランブルキーが設定されている場合には、上記パケットIDによって示されるトランSPORTストリームパケットに含まれるデータエレメントを、設定されたスクランブルキーを使用してスクランブルし、上記パケットIDに対してスクランブルキーが設定されていない場合には、上記パケットIDによって示されるトランSPORTストリームパケットに含まれるデータはスクランブルしないことを特徴とする請求の範囲第52項に記載のプログラム配信システム。

5 6. 上記マルチプレクサシステムは、

上記スクランブルキーを暗号化する第2の暗号化手段と、上記PATパケット、上記PMTパケット、上記CATパケット、上記データエレメントを含んだトランSPORTストリームパケット、上記暗号化EMMパケット及び上記暗号化ECMパケットをそれぞれバッファリングし、上記多重化手段に対してトランSPORTストリームパケットの単位で出力するための複数のバッファ手段とをさらに備えたことを特徴とする請求の範囲第36項に記載のプログラム配信システム。

5 7. 上記マルチプレクサシステムは、

上記データエレメントを含んだトランSPORTストリームパケットをバッファリングするための複数のバッファのバッファ残量を監視し、上記データエレメントを含んだトランSPORTストリームパケットをバッファリングするための複数のバッファのいずれかがオーバーフローしそうなときには、上記EMMパケットをバッファリングするためのバッファからEMMパケット

を上記多重か手段に出力する代わりに、上記オーバフローしそうなバッファから上記データエレメントを含んだトранSPORTストリームパケットを上記多重化手段に出力することを特徴とする請求の範囲第5 6項に記載のプログラム配信システム。

5 8. 上記マルチプレクサシステムから出力されたトランSPORTストリームを、伝送路を介して受信側に配信する配信システムと、

上記伝送路を介して伝送されたトランSPORTストリームを受信する受信システムとをさらに備えていることを特徴とする請求の範囲4 7項に記載のプログラム配信システム。

5 9. 上記受信システムは、

上記伝送されたトランSPORTストリームをデマルチプレクスするデマルチプレクサと、上記スクランブルされた各データエレメントを、供給されたスクランブルキーを使用してそれぞれデスクランブルするデスクランブラーと、

上記デスクランブルされたデータをデータエレメント毎にそれぞれデコードするデコーダと、上記トランSPORTストリームを構成するトランSPORTストリームパケットを解析するC P Uと、上記トランSPORTストリームに含まれる暗号化スクランブルキーを解読し、暗号解読されたスクランブルキーを上記デスクランブラーに供給するセキュリティモジュールと、

を備えたことを特徴とする請求の範囲第5 8項に記載のプログラム配信システム。

6 0. 上記C P Uは、

上記トランSPORTストリームに含まれるプログラムアソシエーションテーブルを解析するP A T解析手段と、

上記トランSPORTストリームに含まれるプログラムマップテーブルを解析す

るPMT解析手段と、上記トランSPORTストリームに含まれるコンディショナルアクセステーブルを解析するCAT解析手段と、

上記トランSPORTストリームに含まれる暗号化EMMデータを解析するEMM解析手段と、上記トランSPORTストリームに含まれる暗号化ECMデータを解析するECM解析手段とを備えていることを特徴とする請求の範囲第59項に記載のプログラム配信システム。

61. 上記セキュリティモジュールは、

上記EMMデータに含まれる自己の契約情報を記憶するメモリ手段と、

上記トランSPORTストリーム中に含まれる暗号化ワークキーと上記顧客管理システムにおいて使用されたマスターキーと同じマスターキーを受取り、上記マスターキーを使用して上記暗号化ワークキーの暗号を解読する第1の暗号解読手段と、

上記トランSPORTストリーム中に含まれる暗号化スクランブルキーと上記第1の暗号解読手段から供給された暗号解読されやワークキーとを受取り、上記暗号解読されたワークキーを使用して上記暗号化スクランブルの暗号を解読する第2の暗号解読手段と、

を備えたことを特徴とする請求の範囲第59項に記載のプログラム配信システム。

62. 上記CPUは、

上記トランSPORTストリームに含まれるプログラムアソシエーションテーブル及びプログラムマップテーブルを解析することによって、上記プログラムを構成する各データエレメントを含んだトランSPORTストリームパケットを識別し、上記データエレメントを含んだトランSPORTストリームパケットを適切な上記スクランブラーにそれぞれ出力するように上記デマルチプレクサを制御する請求の範囲第61項に記載のプログラム配信システム。

6 3. 上記 C P U は、

上記トランSPORTストリームに含まれるコンディショナルアクセステーブルを解析することによって、E MMデータが含まれるトランSPORTストリームパケットを検出し、

上記 E MMデータが含まれるトランSPORTストリームから、受信者が契約しているプログラムに関するE MMデータを有するトランSPORTストリームパケットのみをフィルタリングし、上記フィルタリングされたトランSPORTストリームパケットに含まれるE MMデータを解析することによって、E MMデータから上記暗号化ワークキーを得ることを特徴とする請求の範囲第6 2項に記載のプログラム配信システム。

6 4. 上記 C P U は、

上記トランSPORTストリームに含まれるプログラムアソシエーションテーブル及びこのプログラムアソシエーションテーブルによって指定されたプログラムマップテーブルを解析することによって、上記プログラムを構成する複数のデータエレメント及び上記E CMデータを含んだトランSPORTストリームパケットをそれぞれ検出し、

上記複数のデータエレメントを含んだトランSPORTストリームパケットをそれぞれ上記デスクランプラーに供給すると共に、上記E CMデータを含んだトランSPORTストリームパケットを受け取るように、上記デマルチプレクサを制御することを特徴とする請求の範囲第6 1項に記載のプログラム配信システム。

6 5. 上記 C P U は、

上記デマルチプレクサから供給された暗号化E CMデータを含んだトランSPORTストリームパケットから、受信者が契約しているプログラム又はデータエレメントに関する暗号化E CMデータを有するトランSPORTストリームパケット

のみをフィルタリングし、

上記フィルタリングされたトランSPORTストリームパケットに含まれる暗号化ECMデータを解析することによって、上記暗号化ECMデータから上記暗号化スクランブルキーを得ることを特徴とする請求の範囲第64項に記載のプログラム配信システム。

66. 上記プログラムマップテーブルのシンタックスにおいて、上記プログラム番号と上記暗号化ECMパケットのパケットIDとが対応付けられて記述されている場合には、

上記CPUは、上記パケットIDによって指定された暗号化ECMパケットに含まれている暗号化スクランブルキーを、上記プログラムに対応する暗号化スクランブルキーとして上記セキュリティモジュールに供給し、

上記プログラムマップテーブルのシンタックスにおいて、上記プログラムを構成する複数のデータエレメントと上記複数の暗号化ECMパケットのパケットIDとがそれぞれ対応付けられて記述されている場合には、

上記CPUは、上記複数のパケットIDによって指定された暗号化ECMパケットに含まれるそれぞれ異なる複数のスクランブルキーを、上記複数のデータエレメントに対応する暗号化スクランブルキーとして上記セキュリティモジュールに供給する

ことを特徴とする請求の範囲65項に記載のプログラム配信システム。

67. 上記セキュリティモジュールは、

上記CPUから上記プログラムに対応する暗号化スクランブルキーが供給された場合には、供給された暗号化スクランブルキーの暗号を解読し、上記プログラムを構成する複数のデータエレメントに対応する複数のデスクランブラーに対して同じスクランブルキーをそれぞれ供給し、

上記CPUから上記複数のデータエレメントにそれぞれ対応する複数の暗号化

スクランブルキーが供給された場合には、供給された複数の暗号化スクランブルキーの暗号をそれぞれ解読し、上記複数のデータエレメントのうち契約しているデータエレメントに対応する複数のデスクランブラーに対して、それぞれ異なるスクランブルキーを供給する請求の範囲第 6 6 項に記載のプログラム配信システム。

6 8. 複数のデータエレメントから構成されるプログラムを伝送するプログラム伝送システムにおいて、顧客が契約したプログラム及びデータエレメントのみを視聴できるように、上記プログラムに含まれる複数のデータエレメントをスクランブルする際に使用される複数のスクランブルキーを生成する視聴許可システムと、

上記複数のプログラムに含まれるデータエレメントをそれぞれ符号化し、その符号化データエレメントから構成される符号化ストリームを上記各プログラム毎に生成する符号化システムと、上記符号化手段から各プログラム毎に出力された符号化ストリームを多重化する多重化手段と、上記視聴許可システムにおいて生成されたスクランブルキーに基いて、上記多重化ストリームに含まれる符号化データエレメントに対して各データエレメント毎に選択的にスクランブルをかけるスクランブル手段とを備えたマルチプレクサシステムと、

上記マルチプレクサシステムにおいてマルチプレクサされたストリームを伝送する伝送システムを備えたことを特徴とするプログラム伝送システム。

6 9. 複数のデータエレメントをそれぞれ有した複数のプログラムを伝送するプログラム伝送システムにおいて、

上記データエレメント毎にスクランブルキーを生成するスクランブルキー生成手段と、上記複数のプログラムに含まれるデータエレメントをそれぞれ符号化し、その符号化データエレメントから構成される符号化ストリームを上記各プログラム毎に生成する符号化手段と、

上記符号化手段から各プログラム毎に出力された符号化ストリームを多重化し、多重化ストリームを生成する多重化手段と、
上記スクランブルキー生成手段によって生成されたスクランブルキーに基いて、上記多重化ストリームに含まれる符号化データエレメントに対して各データエレメント毎にスクランブルをかけるスクランブル手段と上記スクランブルがかけられた多重化ストリームを伝送する伝送手段と
を備えたことを特徴とするプログラム伝送システム。

70. 複数のデータエレメントから構成されるプログラムを放送する有料放送システムにおいて、顧客のデータエレメント単位の契約を管理するシステムであって、上記顧客に対して契約したデータエレメントに基いて課金処理を行なう顧客管理システムと、

顧客が契約したデータエレメントのみを視聴できるように、上記データエレメント単位に上記データエレメントをスクランブルするために使用される複数のスクランブルキーを生成する視聴許可システムと、上記複数のプログラムに含まれるデータエレメントをそれぞれ符号化し、その符号化データエレメントから構成される符号化ストリームを上記各プログラム毎に生成する符号化システムと、上記符号化手段から各プログラム毎に出力された符号化ストリームを多重化する多重化手段と、上記視聴許可システムにおいて生成された複数のスクランブルキーに基いて、上記多重化ストリームに含まれる符号化データエレメントに対して各データエレメント毎に選択的にスクランブルをかけるスクランブル手段とを備えたマルチプレクサシステムと、

を備えたことを特徴とする有料放送システム。

71. 複数のデータエレメントから構成されるプログラムを伝送するプログラム伝送方法において、上記顧客が契約したプログラム及びデータエレメントのみを視聴できるように、上記プログラムに含まれる複数のデータエレメントをスクラ

ンブルする際に使用される複数のスクランブルキーを生成するスクランブルキー生成工程と、

上記複数のプログラムに含まれるデータエレメントをそれぞれ符号化し、その符号化データエレメントから構成される符号化ストリームを上記各プログラム毎に生成する符号化工程と、

上記符号化手段から各プログラム毎に出力された複数の符号化ストリームを多重化する多重化工程と、上記生成されたスクランブルキーに基いて、上記多重化ストリームに含まれる符号化データエレメントに対して各データエレメント毎に選択的にスクランブルをかけるスクランブル工程と、を備えたことを特徴とするプログラム伝送方法。

7 2. 上記スクランブルキー生成工程において、

上記スクランブルキーを暗号化するために使用されるワークキーをマスターキーを使用して暗号化し、上記暗号化された暗号化ワークキーと上記顧客を識別するための顧客識別番号とを、暗号化 EMMデータとして出力すると共に、

上記暗号化されたワークキーを識別するためのワークキー識別番号と上記スクランブルキーとを、ECMデータとして出力する

ことを特徴とする請求の範囲第 7 1 項に記載のプログラム伝送方法。

7 3. 上記複数のプログラム、上記プログラムを構成する複数のデータエレメント、上記複数の ECMデータ及び上記複数の EMMデータをどのように多重化するかを示すプログラム仕様情報を生成するプログラム仕様情報生成工程をさらに備え、

上記多重化工程において、この生成されたプログラム使用情報に対応するよう、上記複数のプログラム、上記複数のデータエレメント、上記複数の ECMデータ及び上記複数の EMMデータを多重化することを特徴とする請求の範囲第 7 2 項に記載のプログラム伝送方法。

7 4. 上記スランブルキー生成工程において、上記暗号化 E MMデータ及び上記 E CMデータを、それぞれ、トランSPORTストリームパケットの形態を有した暗号化 E MMパケット及び E CMパケットとして出力し、

上記符号化工程において、上記各符号化されたデータエレメンをトランSPORTストリームパケットの形態を有したエレメンタリパケットとして出力し、

上記プログラム仕様情報生成工程において、上記プログラム仕様情報を、トランSPORTストリームパケットの形態を有した P S I パケットとして出力することを特徴とする請求の範囲第 7 3 項に記載のプログラム伝送方法。

7 5. 上記多重化工程において、上記 E CMデータに含まれるスランブルキーを暗号化する暗号化工程を有することを特徴とする請求の範囲第 7 4 項に記載のプログラム伝送方法。

7 6. 上記スランブルキー生成工程において、

上記ワークキーと、該ワークキーを識別するためのワークキー識別番号とをそれぞれ対応付けたワークキーテーブルを生成することを特徴とする請求の範囲第 7 5 項に記載のプログラム伝送方法。

7 7. 上記多重化工程の上記暗号化工程において、

上記 E CMデータに含まれるワークキー識別番号から、上記ワークキーテーブルを参照することによってワークキーを得、

上記ワークキーテーブルから得られたワークキーを使用して上記 E CMデータに含まれるスランブルキーを暗号化し、

上記第 2 の暗号化回路において暗号化された暗号化スランブルキーを、暗号化 E CMデータとして出力することを特徴とする請求の範囲第 7 6 項に記載のプログラム伝送方法。

7 8 . 上記プログラム仕様情報生成工程において、

上記マルチプレクサシステムにトランSPORTストリームパケットの形態として供給される全てのトランSPORTストリームパケットに対して、上記トランSPORTストリームパケットを識別するためのパケットIDを付与することを特徴とする請求の範囲第77項に記載のプログラム伝送方法。

7 9 . 上記プログラム仕様情報は、

少なくとも、プログラムアソシエーションテーブルと、プログラムマップテーブルと、コンディショナルアクセステーブルとから構成されていることを特徴とする請求の範囲第78項に記載のプログラム伝送方法。

8 0 . 上記プログラム仕様情報生成工程において、

上記プログラムアソシエーションテーブルを含んだトランSPORTストリームパケットをPATパケットとして上記マルチプレクサシステムに供給し、

上記プログラムマップテーブルを含んだトランSPORTストリームパケットをPMTパケットとして上記マルチプレクサシステムに供給し、

上記コンディショナルアクセステーブルを含んだトランSPORTストリームパケットをCATパケットとして上記マルチプレクサシステムに供給することを特徴とする請求の範囲第79項に記載のプログラム伝送方法。

8 1 . 上記プログラムアソシエーションテーブルは、プログラム番号とそのプログラム番号に対応するPMTパケットのパケットIDを指定するためのテーブルであって、

上記プログラムマップテーブルは、プログラムを構成する複数のデータエレメントが含まれるトランSPORTストリームパケットのパケットIDをそれぞれ指定するためのテーブルであって、上記コンディショナルアクセステーブルは、上記暗号化EMMパケットのパケットIDを指定するためのテーブルであることを

特徴とする請求の範囲第 8 0 項に記載のプログラム伝送方法。

8 2. 上記プログラムアソシエーションテーブルには、

プログラムを示すプログラム番号と該プログラムに関連付けられた P M T パケットのパケット I D とが記述され、

上記プログラムマップテーブルには、

上記プログラムを示すプログラム番号と、上記プログラムを構成する複数のデータエレメントが含まれるトランスポートストリームパケットが含まれる複数のパケット I D と、上記プログラム又は上記データエレメントと関連付けられた暗号化 E C M パケットのパケット I D を指定するためのディスクリプタとが記述されている

ことを特徴とする請求の範囲第 8 1 項に記載のプログラム伝送方法。

8 3. 上記プログラムマップテーブル中の上記ディスクリプタが、上記プログラム番号と対応つけられた位置に記述されている場合には、上記ディスクリプタは、上記プログラムを構成する複数のデータエレメントの全てのデータエレメントをスクランブルするためのスクランブルキーを含んだ E C M パケット I D を指定し、

上記プログラムマップテーブル中の上記ディスクリプタが、上記プログラムの各データエレメントと対応付けられた位置にそれぞれ記述されている場合には、上記プログラムを構成する複数のデータエレメントの各データエレメントをそれぞれスクランブルするための複数のスクランブルキーを含んだ複数の E C M パケットのパケット I D を指定することを特徴とする請求の範囲第 8 2 項に記載のプログラム伝送方法。

8 4. 上記プログラムが、第 1 のデータエレメントから第 n のデータエレメントを有し、上記第 1 のデータエレメントから第 n のデータエレメントに対して少な

くとも 1 つの異なるスクランブルキーが指定されている場合には、

上記プログラムマップテーブルにおいて、

第 1 番めのデータエレメントが含まれるトランSPORTストリームパケットのパケット ID と、上記第 1 番めのデータエレメントをスクランブルするスクランブルキーを含んだ ECM データを含んだトランSPORTストリームパケットのパケット ID とが対応付けられて記述され、

第 n 番めのデータエレメントが含まれるトランSPORTストリームパケットのパケット ID と、上記第 n 番めのデータエレメントをスクランブルするスクランブルキーを含んだ ECM データを含んだトランSPORTストリームパケットのパケット ID とが対応付けられて記述されていることを特徴とする請求の範囲第 8 3 項に記載のプログラム伝送方法。

8 5. 上記スクランブル工程において、

上記データエレメントを含んだトランSPORTストリームパケットのパケット ID と上記データエレメントに対して指定されたスクランブルキーとを対応付けた対応テーブルに基いて、上記データエレメントに対して指定されたスクランブルキーを使用して、上記プログラム仕様情報、上記 EMM データ及び上記 ECM データはスクランブルせずに、上記データエレメントのみをそれぞれスクランブルすることを特徴とする請求の範囲第 8 0 項に記載のプログラム伝送方法。

8 6. 上記プログラム仕様情報生成工程において、

各トランSPORTストリームパケットに対して割り当てられたパケット ID と、該トランSPORTストリームパケットに含まれるデータをスクランブルする際に使用するスクランブルキーとを対応付けたテーブルを生成し、

上記パケット ID と上記スクランブルキーとを対応付けたテーブルを、上記マルチプレクサシステムに供給することを特徴とする請求の範囲第 8 0 項に記載のプログラム伝送方法。

8 7. 上記スクランブル手段は、

上記パケット I D と上記スクランブルキーとを対応付けたテーブルを参照することによって、上記プログラム仕様情報、上記 E M M データ及び上記 E C M データはスクランブルせずに、上記データエレメントのみをスクランブルすることを特徴とする請求の範囲第 8 6 項に記載のプログラム伝送方法。

8 8. 上記スクランブル工程において、

上記多重化手段から上記スクランブル手段に供給されたトランSPORTストリームパケットの全てのトランSPORTストリームパケットのパケット I D を検出し、

上記パケット I D と上記スクランブルキーとを対応付けたテーブルに基いて、上記検出されたパケット I D に対してスクランブルキーが設定されているか否かを判断し、

上記パケット I D に対してスクランブルキーが設定されている場合には、上記パケット I D によって示されるトランSPORTストリームパケットに含まれるデータエレメントを、設定されたスクランブルキーを使用してスクランブルし、

上記パケット I D に対してスクランブルキーが設定されていない場合には、上記パケット I D によって示されるトランSPORTストリームパケットに含まれるデータはスクランブルしないことを特徴とする請求の範囲第 8 6 項に記載のプログラム伝送方法。

8 9. 上記多重化工程において、

上記スクランブルキーを上記ワークキーを仕様して暗号化し、

上記 P A T パケット、上記 P M T パケット、上記 C A T パケット、上記データエレメントを含んだトランSPORTストリームパケット、上記暗号化 E M M パケット及び上記暗号化 E C M パケットをそれぞれ複数のバッファ手段にバッファリ

ングすることを特徴とする請求の範囲第 7 4 項に記載のプログラム伝送方法。

9 0. 上記多重化工程において、

上記データエレメントを含んだトランSPORTストリームパケットをバッファリングするための複数のバッファのバッファ残量を監視し、

上記データエレメントを含んだトランSPORTストリームパケットをバッファリングするための複数のバッファのいずれかがオーバーフローしそうなときには、上記EMMパケットをバッファリングするためのバッファからEMMパケットを上記多重化手段に出力する代わりに、上記オーバーフローしそうなバッファから上記データエレメントを含んだトランSPORTストリームパケットを出力することを特徴とする請求の範囲第 8 9 項に記載のプログラム伝送方法。

9 1. プログラム配信システムから配信された複数のプログラム及び上記プログラムを構成する複数のデータエレメントのうち、契約されたプログラム及びデータエレメントのみを限定的に受信する限定受信システムにおいて、

上記トランSPORTストリームから、上記プログラムを構成する複数のスクランブルされたデータエレメントを含んでいるトランSPORTストリームパケットをデマルチプレクスすると共に、上記複数のデータエレメントに対応付けられた複数の暗号化スクランブルキーを含んだ複数のトランSPORTストリームパケットをデマルチプレクスするデマルチプレクサ手段と、

上記デマルチプレクスされた複数の暗号化スクランブルキーを含んだ複数のトランSPORTストリームパケットから、受信者が契約したプログラム及びデータエレメントに関連付けられた暗号化スクランブルキーを含んだトランSPORTストリームパケットをフィルタリングするフィルタ手段と、上記フィルタリングされた複数のトランSPORTストリームパケットに含まれる複数の暗号化スクランブルキーの暗号を解読し、暗号解読された複数のスクランブルキーを生成する暗号解読手段と、上記複数のデータエレメントに対応付けられた複数の暗号解読さ

れたスクランブルキーを使用して、上記デマルチプレクサされた複数のデータエレメントを上記データエレメント毎にデスクランブルするデスクランブル手段と、

上記デスクランブル手段においてデスクランブルされた複数のデータエレメントをそれぞれデコードするデコード手段と
から構成されることを特徴とする限定受信システム。

9 2. 上記プログラム配信システムは、

顧客のプログラム毎及びデータエレメント毎の契約を管理するための顧客管理システムと、上記顧客が契約したプログラム及びデータエレメントのみを視聴できるように、上記プログラムに含まれる複数のデータエレメントをスクランブルする際に使用される複数のスクランブルキーを生成する視聴許可システムと、

上記複数のプログラムに含まれるデータエレメントをそれぞれ符号化し、その符号化データエレメントから構成される符号化ストリームを上記各プログラム毎に生成する符号化システムと、上記符号化手段から各プログラム毎に出力された符号化ストリームを多重化する多重化手段と、上記視聴許可システムにおいて生成されたスクランブルキーに基いて、上記多重化ストリームに含まれる符号化データエレメントに対して各データエレメント毎に選択的にスクランブルをかけるスクランブル手段とを備えたマルチプレクサシステムと、

上記マルチプレクサシステムにおいてマルチプレクサされたストリームを伝送する伝送システムを備えたことを特徴とする請求の範囲第91項に記載の限定受信システム。

9 3. 上記視聴許可システムは、

上記スクランブルキーを暗号化するために使用されるワークキーをマスターキーを使用して暗号化するための第1の暗号化手段を備え、

上記第1の暗号化手段によって暗号化された暗号化ワークキーと上記顧客を識

別するための顧客識別番号とを、暗号化 EMMデータとして上記マルチプレクサシステムに供給し、

上記暗号化手段において暗号化されたワークキーを識別するためのワークキー識別番号と上記スクランブルキーとを、ECMデータとして上記マルチプレクサシステムに供給する

ことを特徴とする請求の範囲第 9 2 項に記載の限定受信システム。

9 4. 上記複数のプログラム、上記プログラムを構成する複数のデータエレメント、上記複数の ECMデータ及び上記複数の EMMデータをどのように多重化するかを示すプログラム仕様情報を生成し、この生成されたプログラム使用情報に対応するように、上記複数のプログラム、上記複数のデータエレメント、上記複数の ECMデータ及び上記複数の EMMデータを多重化するように上記エンコーダシステム及び上記マルチプレクサシステムを制御する、エンコーダ／マルチプレクサコントロールシステムを備えたことを特徴とする請求の範囲第 9 3 項に記載の限定受信システム。

9 5. 上記エンコーダシステムは、上記各符号化されたデータエレメントをそれぞれトランSPORTストリームパケットの形態を有したエレメンタリパケットとして上記マルチプレクサシステムに供給し、上記視聴許可システムは、上記暗号化 EMMデータ及び上記 ECMデータを、それぞれ、トランSPORTストリームパケットの形態を有した暗号化 EMMパケット及び ECMパケットとして上記マルチプレクサシステムに供給し、

上記エンコーダ／マルチプレクサコントロールシステムは、上記プログラム仕様情報を、トランSPORTストリームパケットの形態を有した P S I パケットとして上記マルチプレクサシステムに供給することを特徴とする請求の範囲第 9 4 項に記載の限定受信システム。

9 6. 上記マルチプレクサシステムは、

上記E C Mデータに含まれるスクランブルキーを暗号化するための第2の暗号化手段をさらに備えたことを特徴とする請求の範囲第9 5項に記載の限定受信システム。

9 7. 上記視聴許可システムは、

上記ワークキーと、該ワークキーを識別するためのワークキー識別番号とをそれぞれ対応付けたワークキーテーブルを上記マルチプレクサシステムの上記第2の暗号化手段に供給することを特徴とする請求の範囲第9 6項に記載の限定受信システム。

9 8. 上記第2の暗号化手段は、

上記E C Mデータに含まれるワークキー識別番号から、上記ワークキーテーブルを参照することによってワークキーを得、

上記第2の暗号化手段において、上記ワークキーテーブルから得られたワークキーを使用して上記E C Mデータに含まれるスクランブルキーを暗号化し、

上記第2の暗号化回路において暗号化された暗号化スクランブルキーを、暗号化E C Mデータとして上記多重化手段に供給することを特徴とする請求の範囲第9 7項に記載の限定受信システム。

9 9. 上記エンコーダ／マルチプレクサコントロールシステムは、

上記マルチプレクサシステムにトランSPORTストリームパケットの形態として供給される全てのトランSPORTストリームパケットに対して、上記トランSPORTストリームパケットを識別するためのパケットI Dを付与することを特徴とする請求の範囲第9 8項に記載の限定受信システム。

1 0 0. 上記プログラム仕様情報は、

少なくとも、プログラムアソシエーションテーブルと、プログラムマップテーブルと、コンディショナルアクセステーブルとから構成されていることを特徴とする 40 請求の範囲第 99 項に記載の限定受信システム。

101. 上記エンコーダ／マルチプレクサコントロールシステムは、
上記プログラムアソシエーションテーブルを含んだトランSPORTストリーム
パケットを P A T パケットとして上記マルチプレクサシステムに供給し、
上記プログラムマップテーブルを含んだトランSPORTストリームパケットを
P M T パケットとして上記マルチプレクサシステムに供給し、
上記コンディショナルアクセステーブルを含んだトランSPORTストリームパ
ケットを C A T パケットとして上記マルチプレクサシステムに供給することを特
徴とする請求の範囲第 100 項に記載の限定受信システム。

102. 上記プログラムアソシエーションテーブルは、プログラム番号とそのプロ
グラム番号に対応する P M T パケットのパケット I D を指定するためのテーブ
ルであって、
上記プログラムマップテーブルは、プログラムを構成する複数のデータエレメ
ントが含まれるトランSPORTストリームパケットのパケット I D をそれぞれ指
定するためのテーブルであって、上記コンディショナルアクセステーブルは、上
記暗号化 E M M パケットのパケット I D を指定するためのテーブルであることを
特徴とする請求の範囲第 101 項に記載の限定受信システム。

103. 上記プログラムアソシエーションテーブルには、
プログラムを示すプログラム番号と該プログラムに関連付けられた P M T パケ
ットのパケット I D とが記述され、
上記プログラムマップテーブルには、
上記プログラムを示すプログラム番号と、上記プログラムを構成する複数のデ

ータエレメントが含まれるトランSPORTストリームパケットが含まれる複数のパケットIDと、上記プログラム又は上記データエレメントと関連付けられた暗号化ECMパケットのパケットIDを指定するためのディスクリプタとが記述されている

ことを特徴とする請求の範囲第102項に記載の限定受信システム。

104. 上記プログラムマップテーブル中の上記ディスクリプタが、上記プログラム番号と対応つけられた位置に記述されている場合には、上記ディスクリプタは、上記プログラムを構成する複数のデータエレメントの全てのデータエレメントをスクランブルするためのスクランブルキーを含んだECMパケットのパケットIDを指定し、

上記プログラムマップテーブル中の上記ディスクリプタが、上記プログラムの各データエレメントと対応付けられた位置にそれぞれ記述されている場合には、上記プログラムを構成する複数のデータエレメントの各データエレメントをそれぞれスクランブルするための複数のスクランブルキーを含んだ複数のECMパケットのパケットIDを指定することを特徴とする請求の範囲第103項に記載の限定受信システム。

105. 上記プログラムが、第1のデータエレメントから第nのデータエレメントを有し、上記第1のデータエレメントから第nのデータエレメントに対して少なくとも1つの異なるスクランブルキーが指定されている場合には、

上記プログラムマップテーブルにおいて、

第1番めのデータエレメントが含まれるトランSPORTストリームパケットのパケットIDと、上記第1番めのデータエレメントをスクランブルするスクランブルキーを含んだECMデータを含んだトランSPORTストリームパケットのパケットIDとが対応付けられて記述され、

第n番めのデータエレメントが含まれるトランSPORTストリームパケットの

パケット ID と、上記第 n 番めのデータエレメントをスクランブルするスクランブルキーを含んだ ECM データを含んだトランSPORTストリームパケットのパケット ID とが対応付けられて記述されていることを特徴とする請求の範囲第 104 項に記載の限定受信システム。

106. 上記スクランブル手段は、

上記データエレメントを含んだトランSPORTストリームパケットのパケット ID と上記データエレメントに対して指定されたスクランブルキーとを対応付けた対応テーブルに基いて、上記データエレメントに対して指定されたスクランブルキーを使用して、上記プログラム仕様情報、上記 EMM データ及び上記 ECM データはスクランブルせずに、上記データエレメントのみをそれぞれスクランブルすることを特徴とする請求の範囲第 101 項に記載の限定受信システム。

107. 上記エンコーダ／マルチプレクサコントロールシステムは、

各トランSPORTストリームパケットに対して割り当てられたパケット ID と、該トランSPORTストリームパケットに含まれるデータをスクランブルする際に使用するスクランブルキーとを対応付けたテーブルを生成し、

上記パケット ID と上記スクランブルキーとを対応付けたテーブルを、上記マルチプレクサシステムに供給することを特徴とする請求の範囲第 101 項に記載の限定受信システム。

108. 上記スクランブル手段は、

上記パケット ID と上記スクランブルキーとを対応付けたテーブルを参照することによって、上記プログラム仕様情報、上記 EMM データ及び上記 ECM データはスクランブルせずに、上記データエレメントのみをスクランブルすることを特徴とする請求の範囲第 107 項に記載の限定受信システム。

109. 上記スクランブル手段は、

上記多重化手段から上記スクランブル手段に供給されたトランSPORTストリームパケットの全てのトランSPORTストリームパケットのパケットIDを検出し、

上記パケットIDと上記スクランブルキーとを対応付けたテーブルに基いて、上記検出されたパケットIDに対してスクランブルキーが設定されているか否かを判断し、

上記パケットIDに対してスクランブルキーが設定されている場合には、上記パケットIDによって示されるトランSPORTストリームパケットに含まれるデータエレメントを、設定されたスクランブルキーを使用してスクランブルし、

上記パケットIDに対してスクランブルキーが設定されていない場合には、上記パケットIDによって示されるトランSPORTストリームパケットに含まれるデータはスクランブルしないことを特徴とする請求の範囲第107項に記載の限定受信システム。

110. 上記マルチプレクサシステムは、

上記スクランブルキーを暗号化する第2の暗号化手段と、

上記PATパケット、上記PMTパケット、上記CATパケット、上記データエレメントを含んだトランSPORTストリームパケット、上記暗号化EMMパケット及び上記暗号化ECMパケットをそれぞれバッファリングし、上記多重化手段に対してトランSPORTストリームパケットの単位で出力するための複数のバッファ手段とをさらに備えたことを特徴とする請求の範囲第95項に記載の限定受信システム。

111. 上記マルチプレクサシステムは、

上記データエレメントを含んだトランSPORTストリームパケットをバッファリングするための複数のバッファのバッファ残量を監視し、

上記データエレメントを含んだトランSPORTストリームパケットをバッファリングするための複数のバッファのいずれかがオーバーフローしそうなときには、上記EMMパケットをバッファリングするためのバッファからEMMパケットを上記多重か手段に出力する代わりに、上記オーバーフローしそうなバッファから上記データエレメントを含んだトランSPORTストリームパケットを上記多重化手段に出力することを特徴とする請求の範囲第110項に記載の限定受信システム。

112. 上記フィルタ手段は、

上記トランSPORTストリームに含まれるプログラムアソシエーションテーブルを解析するPAT解析手段と、

上記トランSPORTストリームに含まれるプログラムマップテーブルを解析するPMT解析手段と、上記トランSPORTストリームに含まれるコンディショナルアクセステーブルを解析するCAT解析手段と、

上記トランSPORTストリームに含まれる暗号化EMMデータを解析するEMM解析手段と、上記トランSPORTストリームに含まれる暗号化ECMデータを解析するECM解析手段とを備えていることを特徴とする請求の範囲第109項に記載の限定受信システム。

113. 上記暗号解読手段は、

上記EMMデータに含まれる自己の契約情報を記憶するメモリ手段と、

上記トランSPORTストリーム中に含まれる暗号化ワークキーと上記顧客管理システムにおいて使用されたマスターキーと同じマスターキーを受取り、上記マスターキーを使用して上記暗号化ワークキーの暗号を解読する第1の暗号解読手段と、

上記トランSPORTストリーム中に含まれる暗号化スクランブルキーと上記第1の暗号解読手段から供給された暗号解読されやワークキーとを受取り、上記暗

号解読されたワークキーを使用して上記暗号化スクランブルの暗号を解読する第2の暗号解読手段と、

を備えたことを特徴とする請求の範囲第109項に記載の限定受信システム。

114. 上記デマルチプレクサ手段及び上記フィルタ手段は、

上記トランSPORTストリームに含まれるプログラムアソシエーションテーブル及びプログラムマップテーブルを解析することによって、上記プログラムを構成する各データエレメントを含んだトランSPORTストリームパケットを識別し、上記データエレメントを含んだトランSPORTストリームパケットを適切な上記スクランブラーにそれぞれ出力するように上記デマルチプレクサを制御する請求の範囲第113項に記載の限定受信システム。

115. 上記デマルチプレクサ手段及び上記フィルタ手段は、

上記トランSPORTストリームに含まれるコンディショナルアクセステーブルを解析することによって、EMMデータが含まれるトランSPORTストリームパケットを検出し、

上記EMMデータが含まれるトランSPORTストリームから、受信者が契約しているプログラムに関するEMMデータを有するトランSPORTストリームパケットのみをフィルタリングし、上記フィルタリングされたトランSPORTストリームパケットに含まれるEMMデータを解析することによって、EMMデータから上記暗号化ワークキーを得ることを特徴とする請求の範囲第114項に記載の限定受信システム。

116. 上記デマルチプレクサ手段及び上記フィルタ手段は、

上記トランSPORTストリームに含まれるプログラムアソシエーションテーブル及びこのプログラムアソシエーションテーブルによって指定されたプログラムマップテーブルを解析することによって、上記プログラムを構成する複数のデータ

タエレメント及び上記ECMデータを含んだトランSPORTストリームパケットをそれぞれ検出し、

上記複数のデータエレメントを含んだトランSPORTストリームパケットをそれぞれ上記デスクランプラーに供給すると共に、上記ECMデータを含んだトランSPORTストリームパケットを受け取るように、上記デマルチプレクサを制御することを特徴とする請求の範囲第113項に記載の限定受信システム。

117. 上記デマルチプレクサ手段及び上記フィルタ手段は、

上記デマルチプレクサから供給された暗号化ECMデータを含んだトランSPORTストリームパケットから、受信者が契約しているプログラム又はデータエレメントに関する暗号化ECMデータを有するトランSPORTストリームパケットのみをフィルタリングし、

上記フィルタリングされたトランSPORTストリームパケットに含まれる暗号化ECMデータを解析することによって、上記暗号化ECMデータから上記暗号化スクリプルキーを得ることを特徴とする請求の範囲第116項に記載の限定受信システム。

118. 上記プログラムマップテーブルのシンタックスにおいて、上記プログラム番号と上記暗号化ECMパケットのパケットIDとが対応付けられて記述されている場合には、

上記フィルタ手段は、上記パケットIDによって指定された暗号化ECMパケットに含まれている暗号化スクリプルキーを、上記プログラムに対応する暗号化スクリプルキーとして上記暗号解読手段に供給し、上記プログラムマップテーブルのシンタックスにおいて、上記プログラムを構成する複数のデータエレメントと上記複数の暗号化ECMパケットのパケットIDとがそれぞれ対応付けられて記述されている場合には、

上記フィルタ手段は、上記複数のパケットIDによって指定された暗号化EC

Mパケットに含まれるそれぞれ異なる複数のスクランブルキーを、上記複数のデータエレメントに対応する暗号化スクランブルキーとして上記暗号解読手段に供給する。

ことを特徴とする請求の範囲第117項に記載の限定受信システム。

119. 上記暗号解読手段は、

上記フィルタ手段から上記プログラムに対応する暗号化スクランブルキーが供給された場合には、供給された暗号化スクランブルキーの暗号を解読し、上記プログラムを構成する複数のデータエレメントに対応する複数のデスクランブラーに対して同じスクランブルキーをそれぞれ供給し、

上記フィルタ手段から上記複数のデータエレメントにそれぞれ対応する複数の暗号化スクランブルキーが供給された場合には、供給された複数の暗号化スクランブルキーの暗号をそれぞれ解読し、上記複数のデータエレメントのうち契約しているデータエレメントに対応する複数のデスクランブラーに対して、それぞれ異なるスクランブルキーを供給する請求の範囲第118項に記載の限定受信システム。

120. トランSPORTストリームパケット構成の複数のデータエレメントからなるプログラムデータの上記各トランSPORTストリームパケットを多重化してなる多重化データを受信するデータ受信装置において、

上記データエレメントごとに対応するスクランブルキーを上記多重化データから抽出するスクランブルキー抽出手段と、

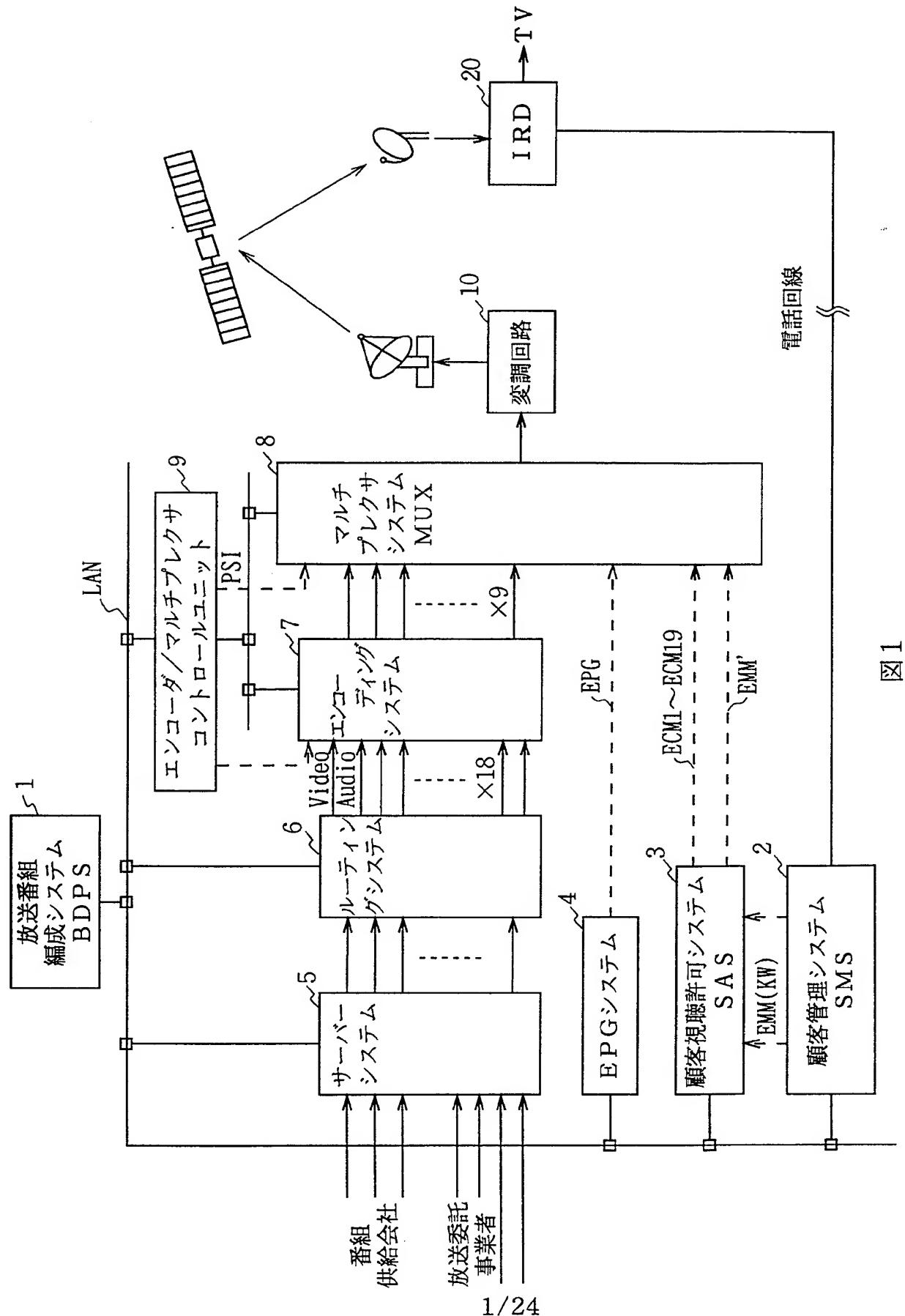
上記スクランブルキー抽出手段によって抽出されたスクランブルキーを用いて上記多重化データに含まれる上記各データエレメントごとのトランSPORTストリームパケットをデスクランブルするデスクランブル手段と
を具えることを特徴とするデータ受信装置。

1 2 1. 上記データ受信装置は、

上記スクランブルキー抽出手段によって抽出された暗号化済の上記スクランブルキーを上記多重化データと共に受信されたワークキーを用いて解読する第1の暗号解読手段を具え、上記第1の暗号解読手段によって解読された上記スクランブルキーを用いて上記トランSPORTストリームパケットをデスクランブルすることを特徴とする請求の範囲第1 2 0 項に記載のデータ受信装置。

1 2 2. 上記データ受信装置は、

上記多重化データと共に受信された暗号化済の上記ワークキーを予め記憶されているマスターキーを用いて解読する第2の暗号解読手段を具え、上記第2の暗号解読手段によって解読された上記ワークキーを用いて上記スクランブルキーを解読することを特徴とする請求の範囲第1 2 0 項に記載のデータ受信装置。



Program number	Video	Main Audio	Sub Audio	Private
1		Ks 1	---	---
2		Ks 2	Ks 3	Ks 4
3	Ks 5	Ks 6	---	---
4	Ks 7	Ks 8	Ks 9	Ks 10
5		Ks 11		
6		Ks 12	---	---
7		Ks 13		Ks 14
8		Ks 15		
9	Ks 16	Ks 17	Ks 18	Ks 19

図 2

P I D値	パケット内に記録される情報
0x0000	P A T
0x0001	C A T
0x0002~0x000F	R e s e r v e d
0x0010	N I T、S T
0x0011	S D T、B A T、S T
0x0012	E I T、S T
0x0013	R S T、S T
0x0014	T D T
0x0015~0x001F	R e s e r v e d
0x0020~0x1FFE	P M T、ビデオ／オーディオ等のストリーム
0x1FFF	N u l l P a c k e t

図3

P I Dテーブル

パケット種類	P I D値	スクランブルキー
P A Tパケット	0×0000 (固定値)	----
⋮	⋮	
⋮	⋮	
⋮	⋮	
P M T 1パケット	0×0100	----
P M T 2パケット	0×0101	----
⋮	⋮	
⋮	⋮	
⋮	⋮	
⋮	⋮	
E C M 1パケット	0×0300	----
⋮	⋮	
E C M 2パケット	0×0351	----
E C M 2パケット	0×0352	----
E C M 3パケット	0×0353	----
E C M 4パケット	0×0354	----
⋮	⋮	
⋮	⋮	
⋮	⋮	
⋮	⋮	
V i d e o [1]パケット	0×0500	K s 1
M a i n _ A u d i o [1]パケット	0×0501	K s 1
V i d e o [2]パケット	0×0502	K s 2
M a i n _ A u d i o [2]パケット	0×0503	K s 2
S u b _ A u d i o [2]パケット	0×0504	K s 3
P r i v a t e [2]パケット	0×0505	K s 4
⋮	⋮	
⋮	⋮	
⋮	⋮	
C A Tパケット	0×0001 (固定値)	----
⋮	⋮	
⋮	⋮	
⋮	⋮	
E M Mパケット	0×0700	----
⋮	⋮	
⋮	⋮	

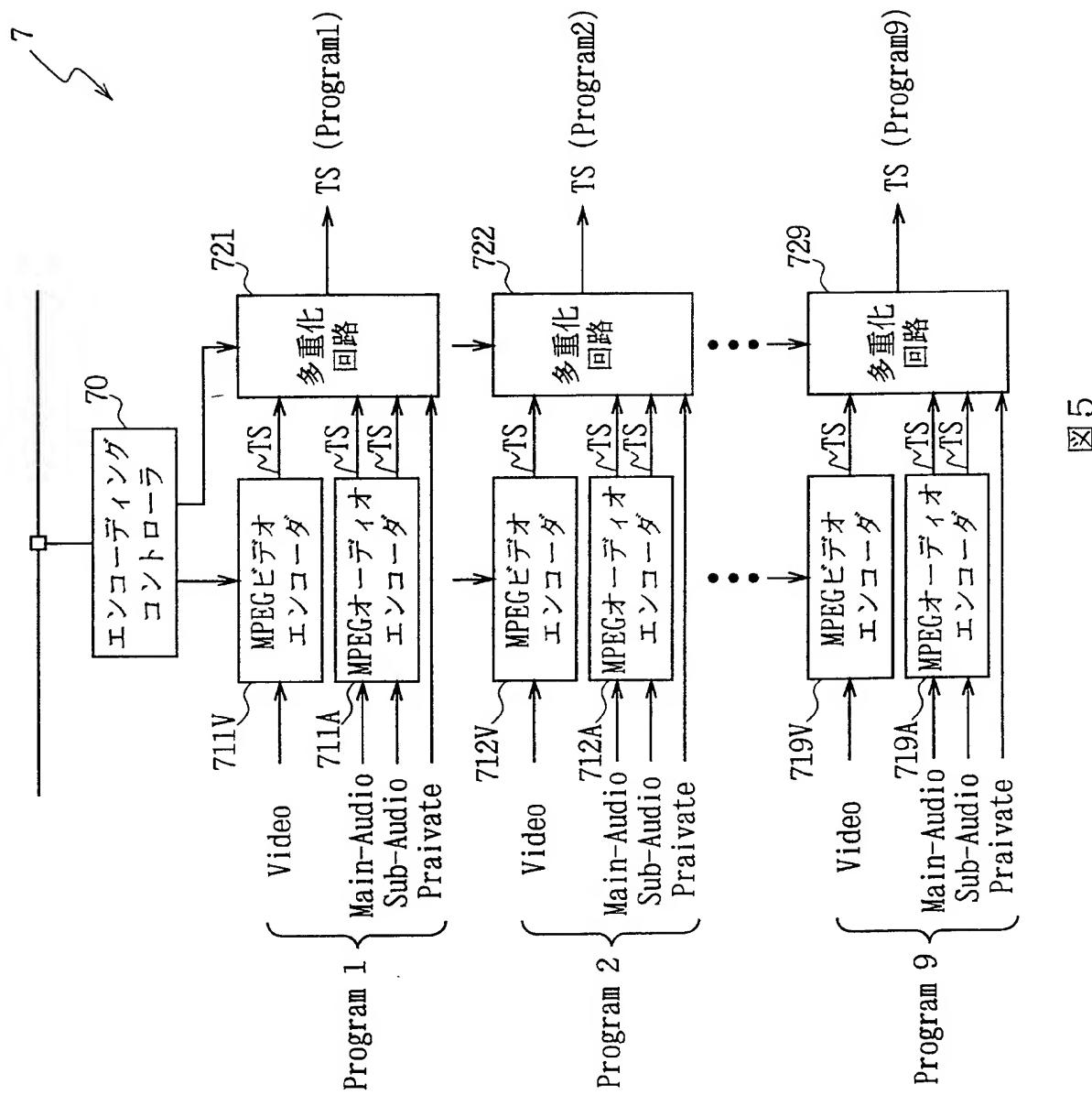


図 5

シンタックス	ビット数	ニーモニック
transport_packet(){		
sync_byte	8	bslbf
transport_error_indicator	1	bslbf
payload_unit_start_indicator	1	bslbf
transport_priority	1	bslbf
PID	13	uimsbf
transport_scrambling_control	2	bslbf
adaptation_field_control	2	bslbf
continuity_counter	4	uimsbf
if(adaptation_field_control=='0' adaptation_field_control=='11'{		
adaptation_field()		
}		
if(adaptation_field_control=='0' adaptation_field_control=='11'{		
for(i=0; i<N; i++){		
data_byte	8	bslbf
}		
}		
}		

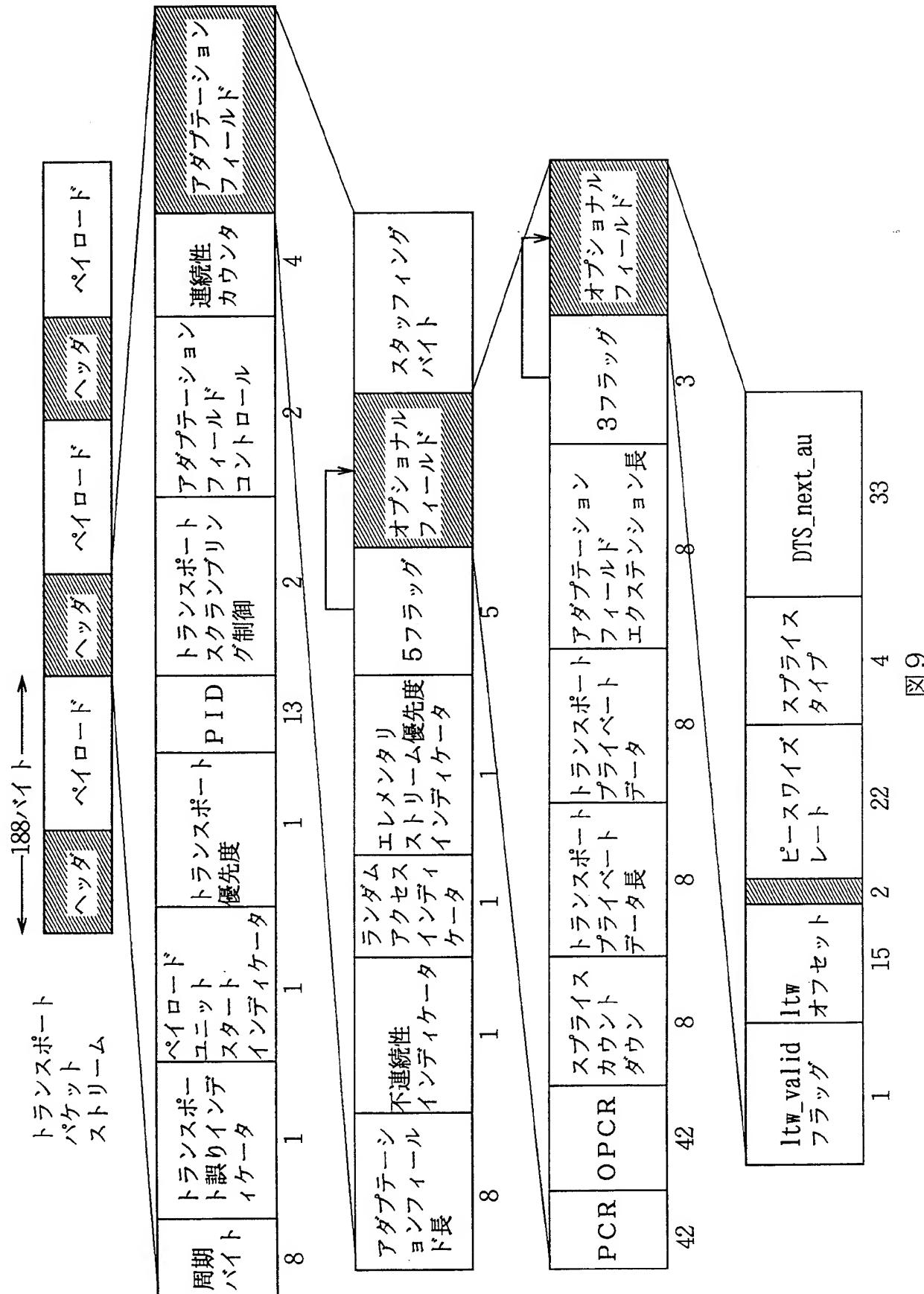
図 6

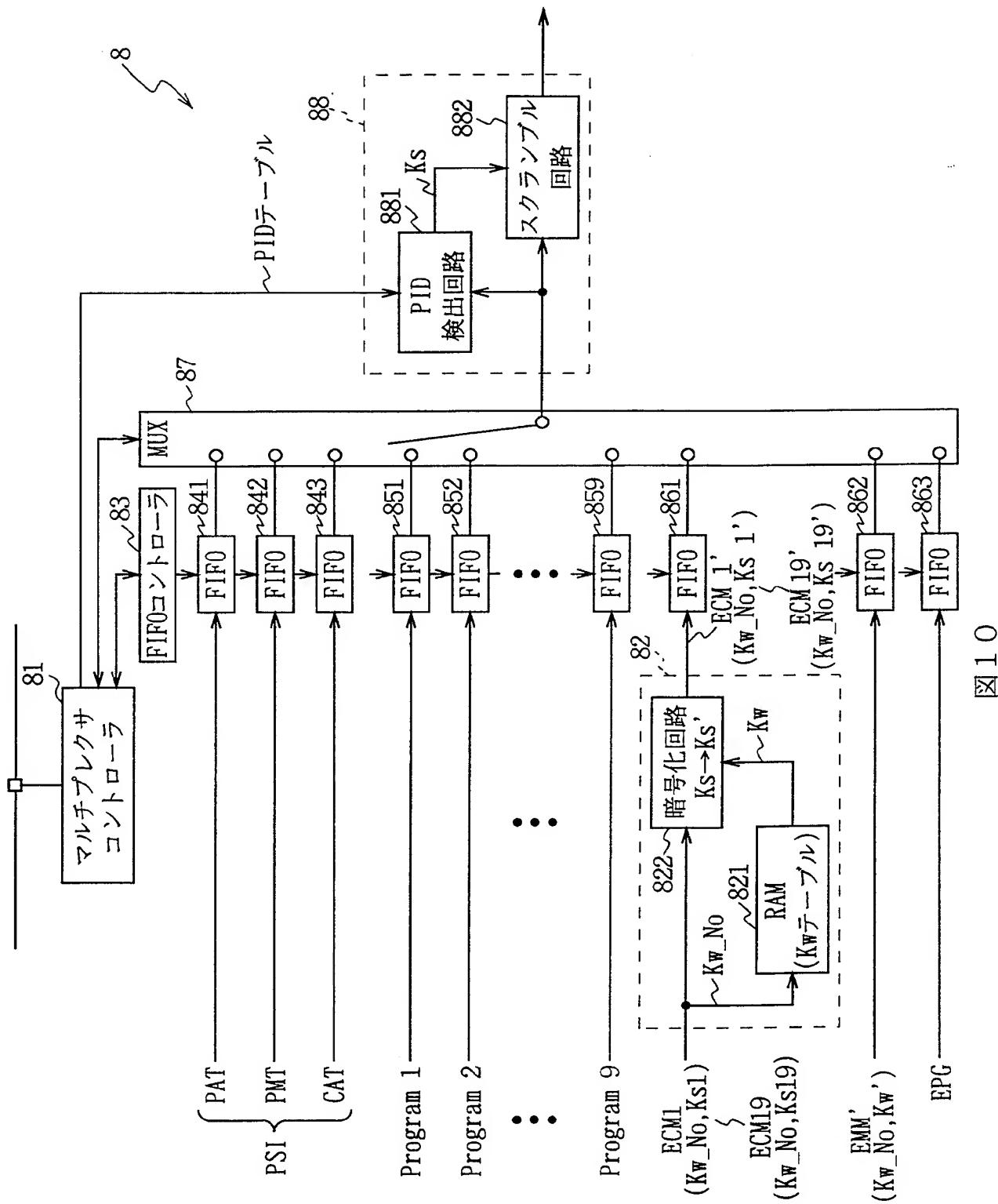
シンタックス	ビット数	ニーモニック
adaptation_field()		
adaptation_field_length	8	uimsbf
if(adaptation_field_length>0){		
discontinuity_indicator	1	bslbf
random_access_indicator	1	bslbf
elementary_stream_priority_indicator	1	bslbf
PCR_flag	1	bslbf
OPCR_flag	1	bslbf
splicing_point_flag	1	bslbf
transport_private_data_flag	1	bslbf
adaptation_field_extension_flag	1	bslbf
if(PCR_flag=='1') {		
program_clock_reference_base	33	uimsbf
reserved	6	bslbf
program_clock_reference_extension	9	uimsbf
}		
if(OPCR_flag=='1') {		
original_program_clock_reference_base	33	uimsbf
reserved	6	bslbf
original_program_clock_reference_extension	9	uimsbf
}		
if(splicing_point_flag=='1') {		
splice_countdown	8	tcimsbf
}		
if(transport_private_data_flag=='1') {		
transport_private_data_length	8	uimsbf
for(i=0; i<transport_private_data_length; i++) {		
private_data_byte	8	bslbf
}		
}		
if(adaptation_field_extension_flag=='1') {		
adaptation_field_extension_length	8	uimsbf
ltw_flag	1	bslbf
piecewise_rate_flag	1	bslbf
seamless_splice_flag	1	bslbf

図7

```
    reserved                                5  bslbf
    if(ltw_flag=='1'){
        ltw_valid_flag                      1  bslbf
        ltw_offset                           15 uimsbf
    }
    if(piecewise_rate_flag=='1'){
        reserved                            2  bslbf
        piecewise_rate                      22 uimsbf
    }
    if(seamless_splice_flag=='1'){
        splice_type                         4  bslbf
        DTS_next_AU[32..30]                  3  bslbf
        market_bit                           1  bslbf
        DTS_next_AU[29..15]                  15 bslbf
        marker_bit                           1  bslbf
        DTS_next_AU[14..0]                   15 bslbf
        marker_bit                           1  bslbf
    }
    for(i=0;i<N;i++){
        reserved                            8  bslbf
    }
}
for(i=0;i<N;i++){
    stuffing_byte                         8  bslbf
}
}
```

図8





構造名	割り当てPID #	説明
プログラム アソシエーション テーブル(PAT)	0x00	プログラム番号とプログラムマップ テーブルPIDを割り当てる
プログラムマップ テーブル(PMT)	PATで割り当てる	一つ以上のプログラムの構成要素の PIDを規定する
網情報テーブル (NIT)	PATで割り当てる	FDM周波数や中継器番号などの 物理的なネットワークパラメータ
条件付きアクセス テーブル(CAT)	0x01	一つ以上の(プライベートの) EMMストリームにそれぞれ 固有のPID値を割り当てる

図 1 1

シンタックス	ビット数	ニーモニック
program_association_section()		
table_id	8	uimsbf
section_syntax_indicator	1	bslbf
'0'	1	bslbf
reserved	2	bslbf
section_length	12	uimsbf
transport_stream_id	16	uimsbf
reserved	2	bslbf
version_number	5	uimsbf
current_next_indicator	1	bslbf
section_number	8	uimsbf
last_section_number	8	uimsbf
for(i=0; i<N; i++) {		
program_number	16	uimsbf
reserved	3	bslbf
if(program number == '0')		
network_PID	13	uimsbf
}		
else {		
program_map_PID	13	uimsbf
}		
}		
CRC32	32	rpchof
}		

図12

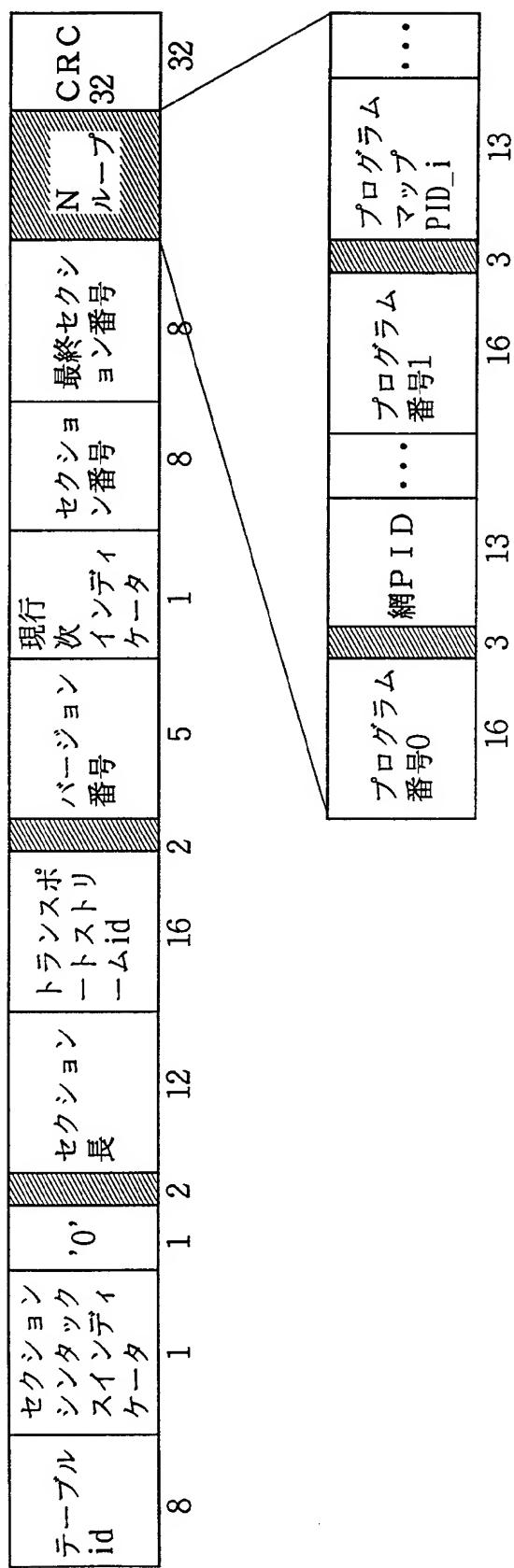


図13

値	説明
0x00	プログラムアソシエーションセクション
0x01	条件付きアクセスセクション(CA section)
0x02	プログラムマップセクション
0x03-0x3F	ITU-T 勧告 H.222.0 ISO/IEC 13818 予約された
0x40-0xFE	ユーザープライベート
0xFF	禁止

図14

シンタックス	ビット数	ニーモニック
TS_program_map_section() {		
table_id	8	uimsbf
section_syntax_indicator	1	bslbf
'0'	1	bslbf
reserved	2	bslbf
section_length	12	uimsbf
program_number	16	uimsbf
reserved	2	bslbf
version_number	5	uimsbf
current_next_indicator	1	bslbf
section_number	8	uimsbf
last_section_number	8	uimsbf
reserved	3	bslbf
PCR_PID	13	uimsbf
reserved	4	bslbf
program_info_length	12	uimsbf
for(i=0; i<N; i++) {		
descriptor()		
}		
for(i=0; i<N; i++) {		
stream_type	8	uimsbf
reserved	3	bslbf
elementary_PID	13	uimsbf
reserved	4	bslbf
ES_info_length	12	uimsbf
for(i=0; i<N2; i++) {		
descriptor()		
}		
}		
CRC32	32	rpchof
}		

図15

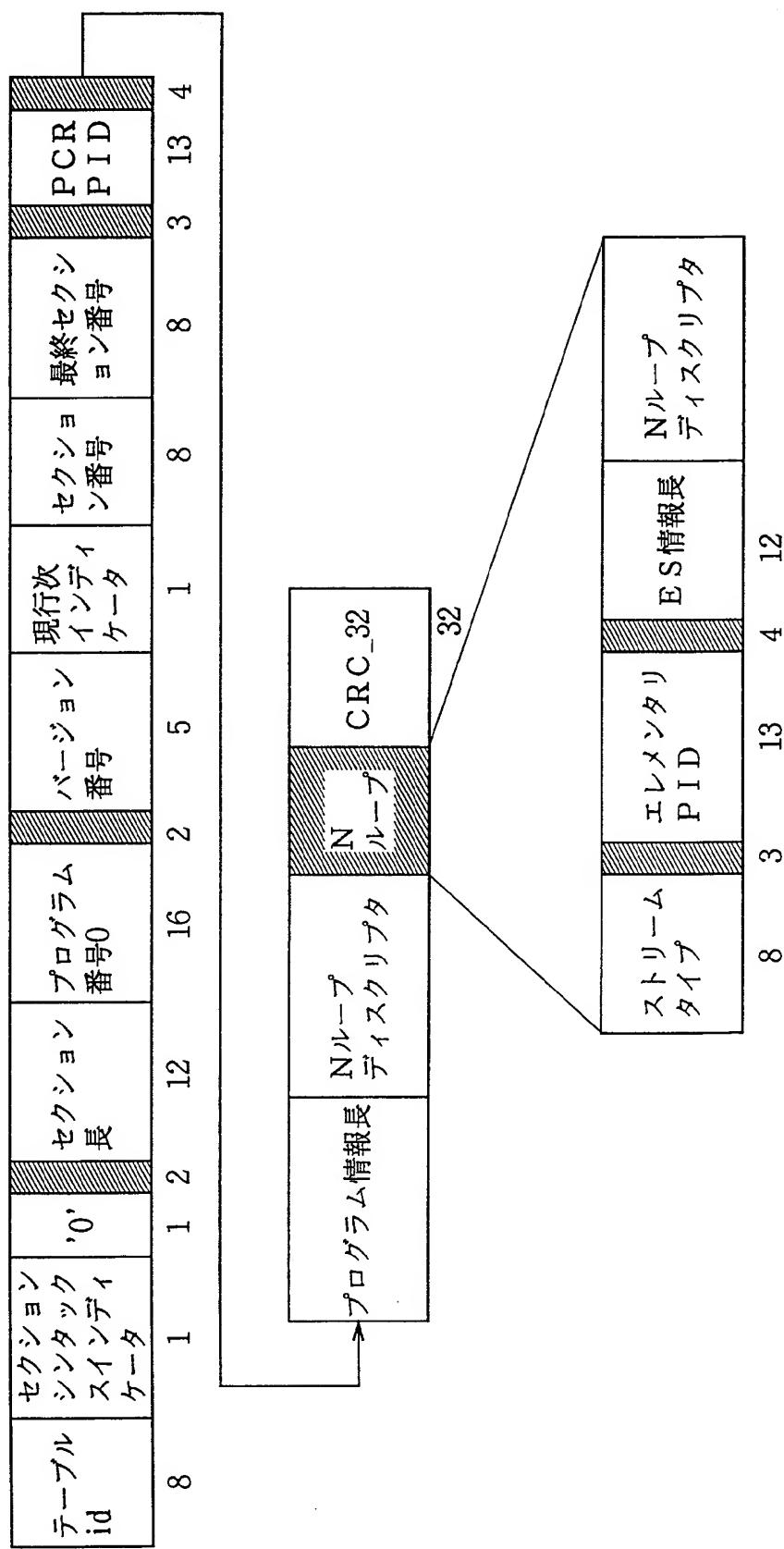


図16

シンタックス	ビット数	ニーモニック
CA_section()		
table_id	8	uimsbf
section_syntax_indicator	1	bslbf
'0'	1	bslbf
reserved	2	bslbf
section_length	12	uimsbf
reserved	18	bslbf
version_number	5	uimsbf
current_next_indicator	1	bslbf
section_number	8	uimsbf
last_section_number	8	uimsbf
for(i=0; i<N; i++) {		
descriptor()		
}		
CRC32	32	rpchof
}		

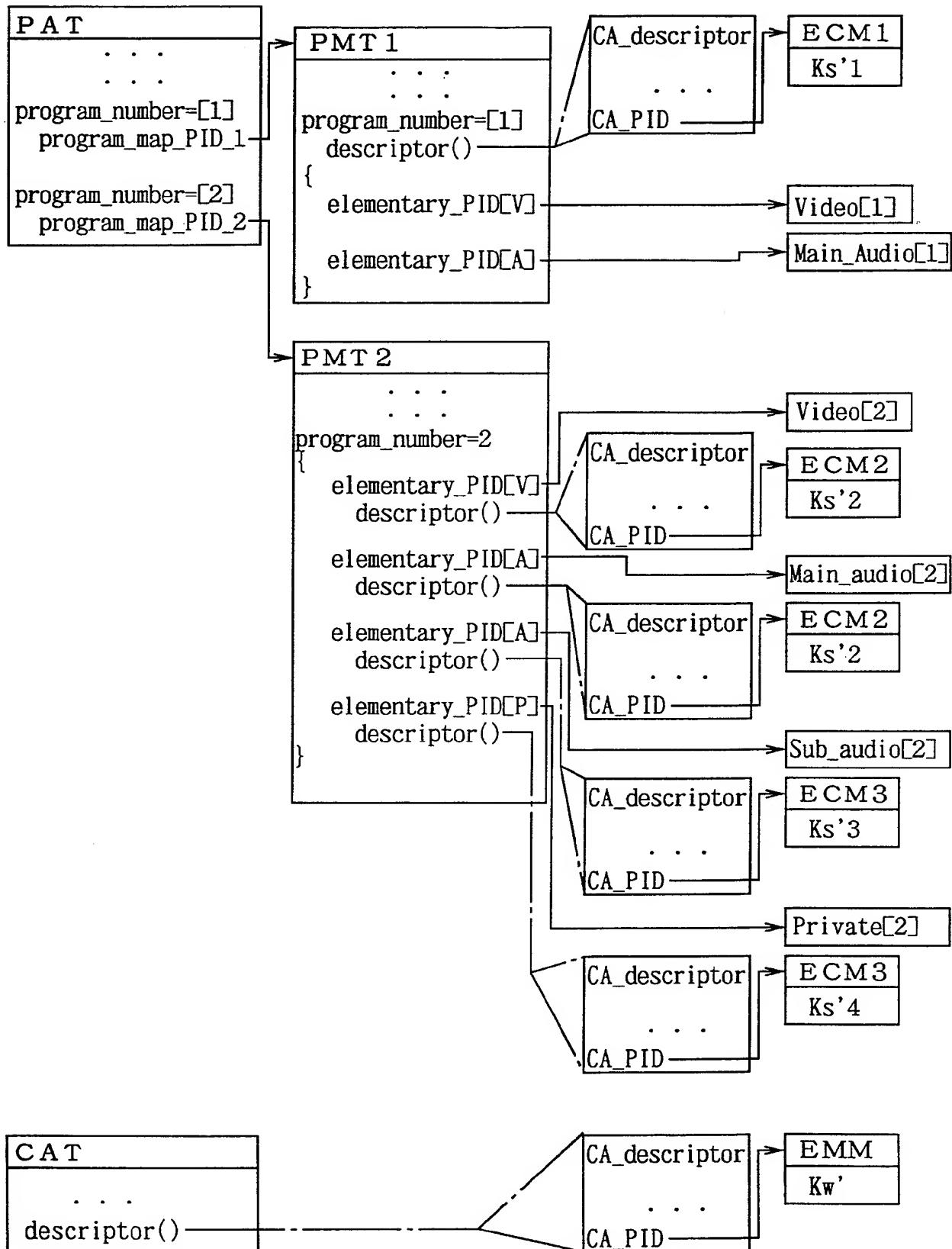
図17

テープル id	セクション シンタック スインタ ケータ	'0'	セクション 長	バージョン 番号	現行次 インデイ ケータ	セクシヨ ン番号	最終セクシ ヨン番号	Nループ ディスク リプタ	CRC 32
8	1	1	2	12	18	5	1	8	8

図18

シンタックス	ビット数	ニーモニック
CA_descriptor()		
descriptor_tag	8	uimbf
descriptor_length	8	uimsbf
CA_system_ID	16	uimsbf
reserved	3	bslbf
CA_PID	13	uimsbf
for(i=0; i<N; i++) {		
private_data_byte	8	uimsbf
}		
}		

図19



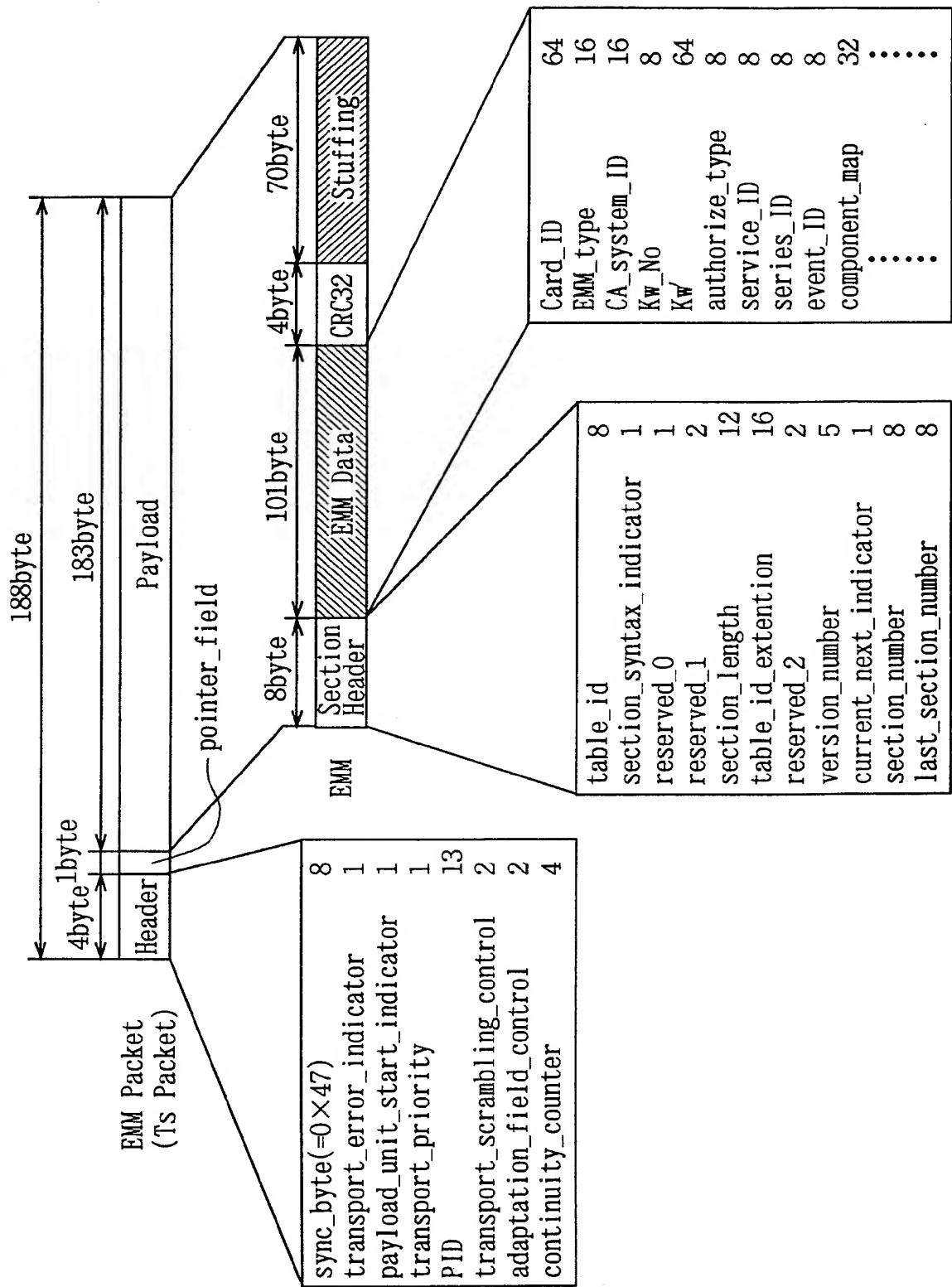


图 2.1

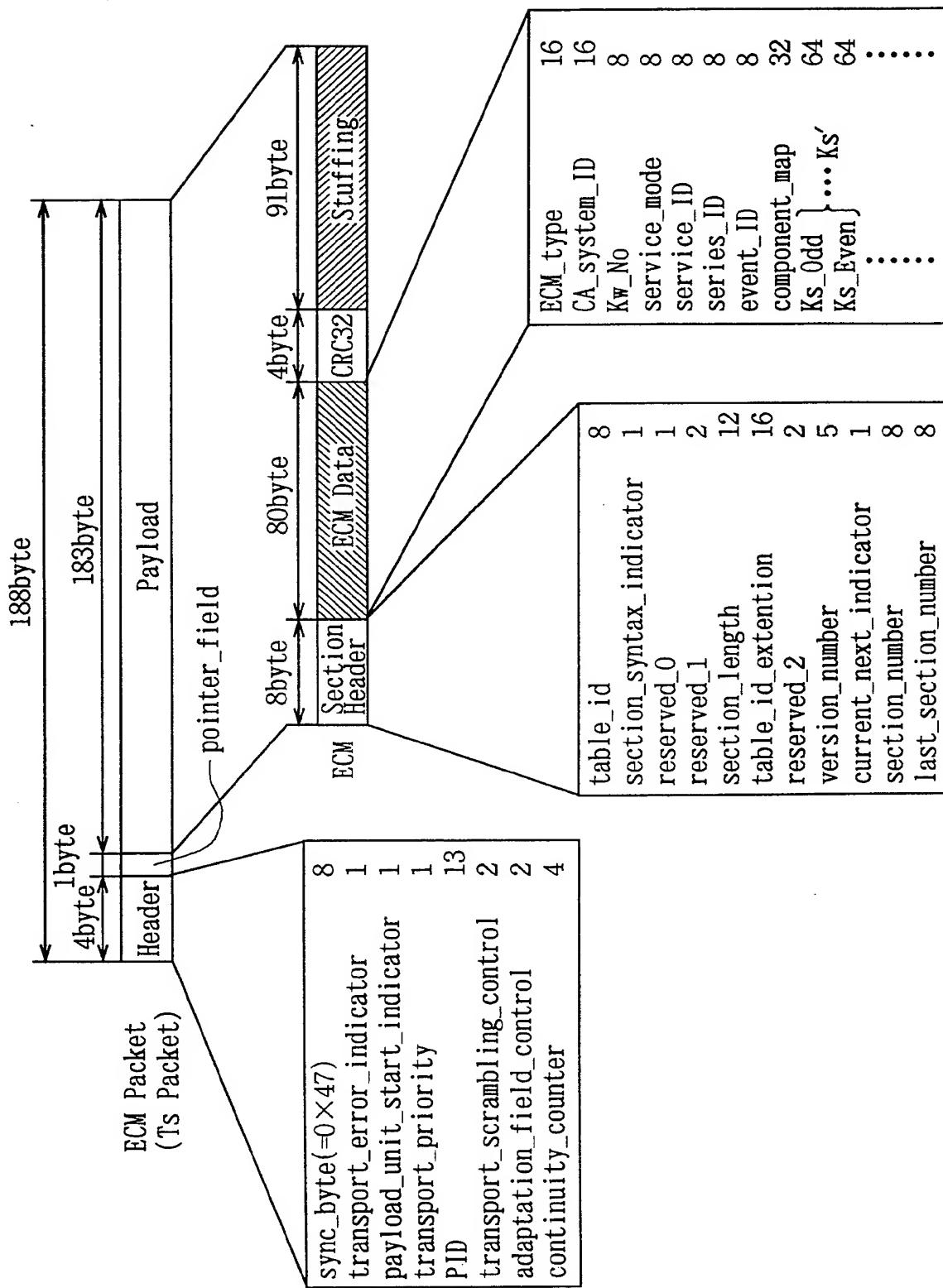
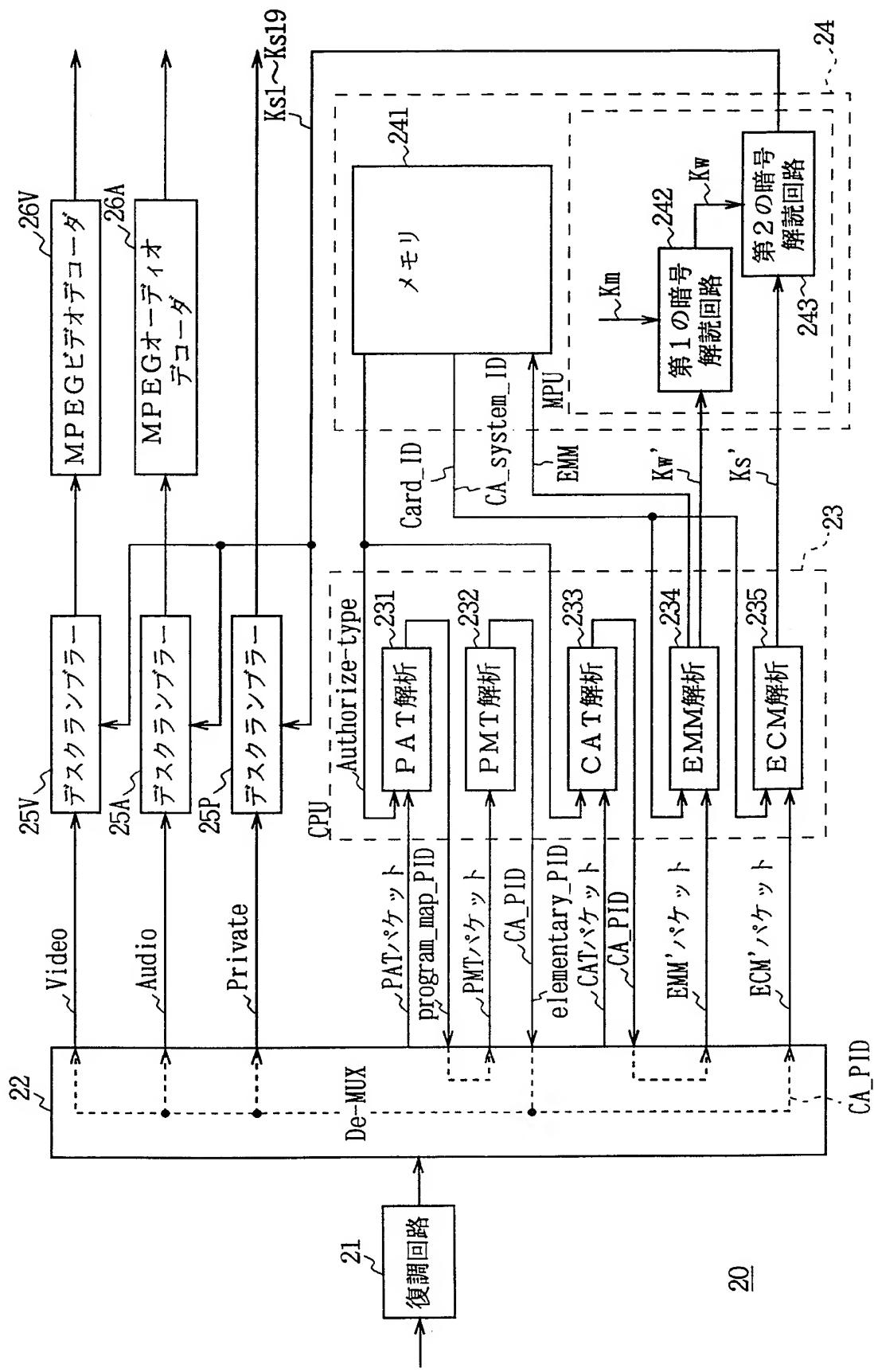


图 22



符 号 の 説 明

1 ……放送番組編成システム、2 ……顧客管理システム、3 ……顧客視聴許可システム、4 ……E P Gシステム、5 ……サーバーシステム、6 ……ルーティングシステム、7 ……エンコーディングシステム、8 ……マルチプレクサシステム、9 ……エンコーダ／エルチプレクサコントロールユニット、10 ……変調回路、20 ……I R D、21 ……復調回路、22 ……デマルチプレクサ、24 ……I Cカード、25 V、25 A、25 P ……デフクランプラー、26 V ……M P E Gビデオデコーダ、26 A ……M P E Gオーディオデコーダ、70 ……エンコーディングコントローラ、241 ……メモリ、242 ……第1の暗号解読回路、243 ……第2の暗号解読回路、711 V～719 V ……M P E Gビデオエンコーダ、711 A～719 A ……M P E Gオーディオエンコーダ、721～729 ……多重化回路、841～863 ……バッファメモリ（F I F O）。

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP98/03127

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl⁶ H04N7/16, 7/167, 08, H04K1/04, H04L12/18

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl⁶ H04N7/16, 7/167, 08, H04K1/04, H04L12/18

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1937-1996 Jitsuyo Shinan Toroku Koho 1996-1998
Kokai Jitsuyo Shinan Koho 1971-1998

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP, 9-511369, A (Scientific Atlanta, Inc.), 11 November, 1997 (11. 11. 97) & WO, 95/26597, A1 & AU, 9472209, A & AU, 687844, B & US, 5420866, A	1-7, 12-26, 28-56, 58-89, 91-110, 112-122
A		8-11, 27, 57, 90, 111
Y	JP, 8-340541, A (Sony Corp.), 24 December, 1996 (24. 12. 96) (Family: none)	1-7, 12-26, 28-56, 58-89, 91-110, 112-122
A		8-11, 27, 57, 90, 111
Y	JP, 9-51520, A (Sony Corp.), 18 February, 1997 (18. 02. 97) (Family: none)	1-7, 12-26, 28-56, 58-89, 91-110, 112-122

Further documents are listed in the continuation of Box C.

See patent family annex.

* Special categories of cited documents:	
"A" document defining the general state of the art which is not considered to be of particular relevance	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"E" earlier document but published on or after the international filing date	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"O" document referring to an oral disclosure, use, exhibition or other means	"&" document member of the same patent family
"P" document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search
7 October, 1998 (07. 10. 98)

Date of mailing of the international search report
20 October, 1998 (20. 10. 98)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP98/03127

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A		8-11, 27, 57, 90, 111
Y	JP, 9-284763, A (Sony Corp.),	8, 9
A	31 October, 1997 (31. 10. 97) (Family: none)	1-7, 10-122
Y	JP, 9-312625, A (Sony Corp.),	8, 9
A	2 December, 1997 (02. 12. 97) (Family: none)	1-7, 10-122
Y	JP, 10-126371, A (Sony Corp.),	8, 9
A	15 May, 1998 (15. 05. 98) (Family: none)	1-7, 10-122
A	JP, 7-202884, A (Sony Corp.),	1-122
	4 August, 1995 (04. 08. 95) (Family: none)	
A	JP, 8-289277, A (Sony Corp.),	1-122
	1 November, 1996 (01. 11. 96) (Family: none)	
A	JP, 8-340514, A (Sony Corp.),	1-122
	24 December, 1996 (24. 12. 96) (Family: none)	
A	JP, 9-9241, A (Sony Corp.),	1-122
	10 January, 1997 (10. 01. 97) (Family: none)	
A	JP, 9-46672, A (Sony Corp.),	1-122
	14 February, 1997 (14. 02. 97) (Family: none)	
A	JP, 9-46681, A (Sony Corp.),	1-122
	14 February, 1997 (14. 02. 97) (Family: none)	
A	JP, 9-284762, A (Sony Corp.),	1-122
	31 October, 1997 (31. 10. 97) (Family: none)	
A	JP, 9-307542, A (Sony Corp.),	1-122
	28 November, 1997 (28. 11. 97) (Family: none)	
A	JP, 9-322161, A (K.K. Ekushingu),	1-122
	12 December, 1997 (12. 12. 97) (Family: none)	

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP98/03127

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

The group of inventions disclosed in claims 1-7 and 12-122 relates to encryption of data elements, whereas the group of inventions disclosed in claims 8-11 relates to time division multiplexing of data elements, and these two groups of inventions are not considered as relating to a group of inventions so linked as to form a single general inventive concept.

1. As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.
3. As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest The additional search fees were accompanied by the applicant's protest.
 No protest accompanied the payment of additional search fees.

国際調査報告

国際出願番号 PCT/JP98/03127

A. 発明の属する分野の分類(国際特許分類(IPC))

Int cl^o H04N7/16, 7/167, 08, H04K1/04, H04L12/18

B. 調査を行った分野

調査を行った最小限資料(国際特許分類(IPC))

Int cl^o H04N7/16, 7/167, 08, H04K1/04, H04L12/18

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1937-1996年
日本国公開実用新案公報	1971-1998年
日本国実用新案登録公報	1996-1998年

国際調査で使用した電子データベース(データベースの名称、調査に使用した用語)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	J P, 9-511369, A (サイエンティフィクーアトランタ・ インコーポレーテッド), 11. 11月. 1997 (11. 11. 97) & WO, 95/26597, A1 & AU, 9472209, A & AU, 687844, B & US, 5420866, A	1-7, 12-26, 28-56, 58-89, 91-110, 112-122
A		8-11, 27, 57, 90, 111

 C欄の続きにも文献が列挙されている。 パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの

「E」先行文献ではあるが、国際出願日以後に公表されたもの

「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献(理由を付す)

「O」口頭による開示、使用、展示等に言及する文献

「P」国際出願目前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&」同一パテントファミリー文献

国際調査を完了した日

07.10.98

国際調査報告の発送日

20.10.98

国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)

郵便番号 100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官(権限のある職員)

山崎 達也

5C 8121

電話番号 03-3581-1101 内線 3541

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	J P, 8-340541, A (ソニー株式会社), 24. 12月. 1996 (24. 12. 96) (ファミリーなし)	1-7, 12-26, 28-56, 58-89, 91-110, 112-122
A		8-11, 27, 57, 90, 111
Y	J P, 9-51520, A (ソニー株式会社), 18. 2月. 19 97 (18. 02. 97) (ファミリーなし)	1-7, 12-26, 28-56, 58-89, 91-110, 112-122
A		8-11, 27, 57, 90, 111
Y A	J P, 9-284763, A (ソニー株式会社), 31. 10月. 1997 (31. 10. 97) (ファミリーなし)	8, 9 1-7, 10-122
Y A	J P, 9-312625, A (ソニー株式会社), 2. 12月. 1 997 (02. 12. 97) (ファミリーなし)	8, 9 1-7, 10-122
Y A	J P, 10-126371, A (ソニー株式会社), 15. 5月. 1998 (15. 05. 98) (ファミリーなし)	8, 9 1-7, 10-122
A	J P, 7-202884, A (ソニー株式会社), 4. 8月. 19 95 (04. 08. 95) (ファミリーなし)	1-122
A	J P, 8-289277, A (ソニー株式会社), 1. 11月. 1 996 (01. 11. 96) (ファミリーなし)	1-122
A	J P, 8-340514, A (ソニー株式会社), 24. 12月. 1996 (24. 12. 96) (ファミリーなし)	1-122
A	J P, 9-9241, A (ソニー株式会社), 10. 1月. 199 7 (10. 01. 97) (ファミリーなし)	1-122
A	J P, 9-46672, A (ソニー株式会社), 14. 2月. 19 97 (14. 02. 97) (ファミリーなし)	1-122
A	J P, 9-46681, A (ソニー株式会社), 14. 2月. 19 97 (14. 02. 97) (ファミリーなし)	1-122
A	J P, 9-284762, A (ソニー株式会社), 31. 10月. 1997 (31. 10. 97) (ファミリーなし)	1-122
A	J P, 9-307542, A (ソニー株式会社), 28. 11月. 1997 (28. 11. 97) (ファミリーなし)	1-122
A	J P, 9-322161, A (株式会社エクシング), 12. 12 月. 1997 (12. 12. 97) (ファミリーなし)	1-122

第I欄 請求の範囲の一部の調査ができないときの意見（第1ページの1の続き）

法第8条第3項（PCT第17条(2)(a)）の規定により、この国際調査報告は次の理由により請求の範囲の一部について作成しなかった。

1. 請求の範囲 _____ は、この国際調査機関が調査をすることを要しない対象に係るものである。つまり、
2. 請求の範囲 _____ は、有意義な国際調査をすることができる程度まで所定の要件を満たしていない国際出願の部分に係るものである。つまり、
3. 請求の範囲 _____ は、従属請求の範囲であってPCT規則6.4(a)の第2文及び第3文の規定に従って記載されていない。

第II欄 発明の単一性が欠如しているときの意見（第1ページの2の続き）

次に述べるようにこの国際出願に二以上の発明があるとこの国際調査機関は認めた。

請求の範囲1-7、12-122はデータエレメントの暗号化に関するものであり、請求の範囲8-11はデータエレメントの時分割多重化時のバッファリングに関するものであり、これら2つの発明群が単一の一般的発明概念を形成するように関連している一群の発明であるとは認められない。

1. 出願人が必要な追加調査手数料をすべて期間内に納付したので、この国際調査報告は、すべての調査可能な請求の範囲について作成した。
2. 追加調査手数料を要求するまでもなく、すべての調査可能な請求の範囲について調査することができたので、追加調査手数料の納付を求めなかった。
3. 出願人が必要な追加調査手数料を一部のみしか期間内に納付しなかったので、この国際調査報告は、手数料の納付のあった次の請求の範囲のみについて作成した。
4. 出願人が必要な追加調査手数料を期間内に納付しなかったので、この国際調査報告は、請求の範囲の最初に記載されている発明に係る次の請求の範囲について作成した。

追加調査手数料の異議の申立てに関する注意

追加調査手数料の納付と共に出願人から異議申立てがあった。
 追加調査手数料の納付と共に出願人から異議申立てがなかった。